Apacer

Apacer TCG SSD SV240 Series

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

August 15, 2022

Version 1.1

Apacer Technology Inc.
1F, No.32, Zhongcheng Rd., Tucheng Dist., New Taipei City, Taiwan, R.O.C
Tel: +886-2-2267-8000 Fax: +886-2-2267-2261
www.apacer.com

Table of Contents

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

List of Tables

List of Figures

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

1. Introduction

This document defines the Security Policy for Apacer Technology Inc. (Apacer) TCG SSD SV240 Series, hereafter referred to as the “Apacer SV240 SSD” or “Module”. The Apacer SV240 SSD is a multi-chip embedded device which provides AES 256 encryption/decryption of data that is stored in NAND flash. The Module supports the SATA interface and is compliant with the Trusted Computing Group (TCG) SSC specification Opal. The Module meets FIPS 140-2 overall Security Level 2 requirements.

Table 1 – Cryptographic Module Configurations

Module	Capacity	Hardware P/N	Firmware Version
SV240-25	120GB	A12.A25HGF	SFYCA11S SFYCA31S
		A12.A25HHF	
	128GB	A12.A22HGF	SFYCA01S SFYCA21S
		A12.A22HHF	
	240GB	A12.A25JGF	SFYCA11S SFYCA31S
		A12.A25JHF	
	256GB	A12.A22JGF	SFYCA01S SFYCA21S
		A12.A22JHF	
	480GB	A12.A25KGF	SFYCA11S SFYCA31S
		A12.A25KHF	
	512GB	A12.A22KGF	SFYCA01S SFYCA21S
		A12.A22KHF	
	960GB	A12.A25LGF	SFYCA11S SFYCA31S
		A12.A25LHF	
	1TB	A12.A23AGF	SFYCA01S SFYCA21S
		A12.A23AHF	
	1920GB	A12.A25MGF	SFYCA11S SFYCA31S
		A12.A25MHF	
	2TB	A12.A23BGF	SFYCA01S SFYCA21S
		A12.A23BHF	
SV240-297	120GB	A92.A25HGA	SFYCA11S SFYCA31S
		A92.A25HHA	
	128GB	A92.A22HGA	SFYCA01S SFYCA21S
		A92.A22HHA	
	240GB	A92.A25JGA	SFYCA11S SFYCA31S
		A92.A25JHA	
	256GB	A92.A22JGA	SFYCA01S SFYCA21S
		A92.A22JHA	
	480GB	A92.A25KGA	SFYCA11S SFYCA31S
		A92.A25KHA	
	512GB	A92.A22KGA	SFYCA01S SFYCA21S
		A92.A22KHA	
	960GB	A92.A25LGA	SFYCA11S SFYCA31S
		A92.A25LHA	
	1TB	A92.A23AGA	SFYCA01S SFYCA21S
		A92.A23AHA	

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Module	Capacity	Hardware P/N	Firmware Version
SV240-300	120GB	A72.A25HGA	SFYCA11S SFYCA31S
		A72.A25HHA	
	128GB	A72.A22HGA	SFYCA01S SFYCA21S
		A72.A22HHA	
	240GB	A72.A25JGA	SFYCA11S SFYCA31S
		A72.A25JHA	
	256GB	A72.A22JGA	SFYCA01S SFYCA21S
		A72.A22JHA	
	480GB	A72.A25KGA	SFYCA11S SFYCA31S
		A72.A25KHA	
	512GB	A72.A22KGA	SFYCA01S SFYCA21S
		A72.A22KHA	
	960GB	A72.A25LGA	SFYCA11S SFYCA31S
		A72.A25LHA	
	1TB	A72.A23AGA	SFYCA01S SFYCA21S
		A72.A23AHA	
	1920GB	A72.A25MGA	SFYCA11S SFYCA31S
		A72.A25MHA	
	2TB	A72.A23BGA	SFYCA01S SFYCA21S
		A72.A23BHA	
SV240-M280	120GB	A52.A25HGB	SFYCA11S SFYCA31S
		A52.A25HHB	
	128GB	A52.A22HGB	SFYCA01S SFYCA21S
		A52.A22HHB	
	240GB	A52.A25JGB	SFYCA11S SFYCA31S
		A52.A25JHB	
	256GB	A52.A22JGB	SFYCA01S SFYCA21S
		A52.A22JHB	
	480GB	A52.A25KGB	SFYCA11S SFYCA31S
		A52.A25KHB	
	512GB	A52.A22KGB	SFYCA01S SFYCA21S
		A52.A22KHB	
	960GB	A52.A25LGB	SFYCA11S SFYCA31S
		A52.A25LHB	
	1TB	A52.A23AGB	SFYCA01S SFYCA21S
		A52.A23AHB	
	1920GB	A52.A25MGB	SFYCA11S SFYCA31S
		A52.A25MHB	
	2TB	A52.A23BGB	SFYCA01S SFYCA21S
		A52.A23BHB	

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated storage devices. The Module is a multi-chip embedded embodiment.

The FIPS 140-2 security levels for the Module are as follows:

Table 2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State 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

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

1.1 Hardware and Physical Cryptographic Boundary

The Apacer SV240 SSD is provided in four physical form factors: 2.5”, M.2, JEDEC MO-297 and MO-300. These are depicted in Figures 1, 2, 3 and 4 below. In these figures the red outline depicts the physical cryptographic boundary.

For the 2.5” form factor, the multi-chip embedded cryptographic module consists of hardware and firmware components that are all enclosed in two aluminum alloy cases, which serve as the cryptographic boundary of the Module. As indicated in Figure 1, the top and bottom cases are assembled by four screws and two tamper-evident labels are applied for the detection of any opening of the cases. No security relevant component can be seen within the visible spectrum through the opaque enclosure. The only components exposed are the SATA Data and Power ports. The Module does not support a maintenance access interface. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this Module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Figure 1 – Apacer SV240 2.5” Form Factor

For the M.2, MO-297 and MO-300 formats, the boundary encompasses the entire PCB. This boundary includes all components (processor and memory) that implement cryptography and process the CSPs. All modules rely on the SATA IO module as input/output devices.

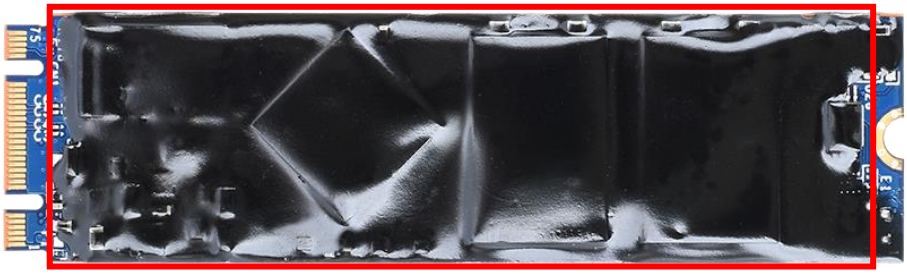

Figure 2 – Apacer SV240 M.2 Form Factor

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

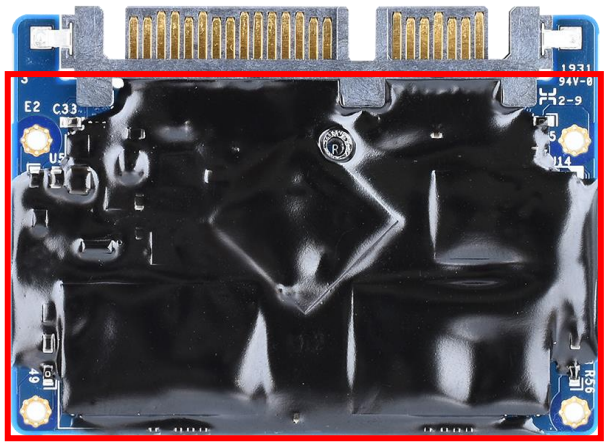

Figure 3 – Apacer SV240 MO-297 Form Factor

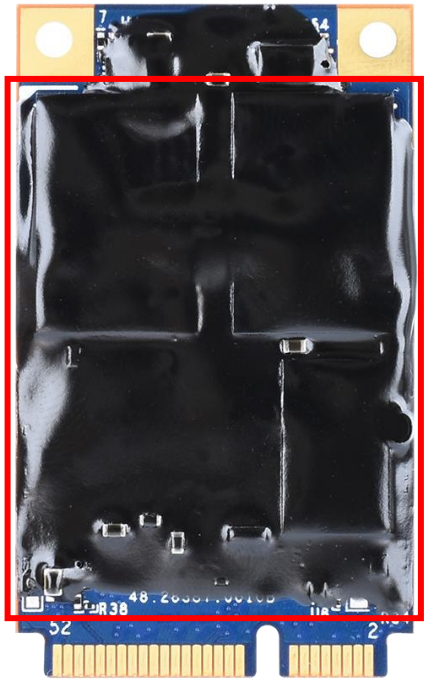

Figure 4 – Apacer SV240 MO-300 Form Factor

The physical ports and logical interfaces are identified in Table 3 below:

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
SATA Power	SATA power	Power In
SATA Data	SATA DATA IO	Control In, Data In, Data Out and Status Out

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

1.2 Logical Cryptographic Boundary

The Apacer SV240 SSD uses a single chip controller with a SATA interface on the system side and Apacer NAND flash internally. The following figure depicts the Module operational environment. The red outline in the figure depicts the logical cryptographic boundary which is within the enclosure of the device. All firmware runs on the controller within this logical boundary.

The Module is composed of the following components:

- Host interface: Provides control status and data paths.
- SSD controller: All firmware and software executes on the controller which provides SATA host interface.
- DDR: Provides data mapping tables and buffer for user data going into and out of the device.
- NAND flash: Storage medium where user data, system data, mapping tables, and main firmware are stored.

Figure 5 depicts the Module block diagram.

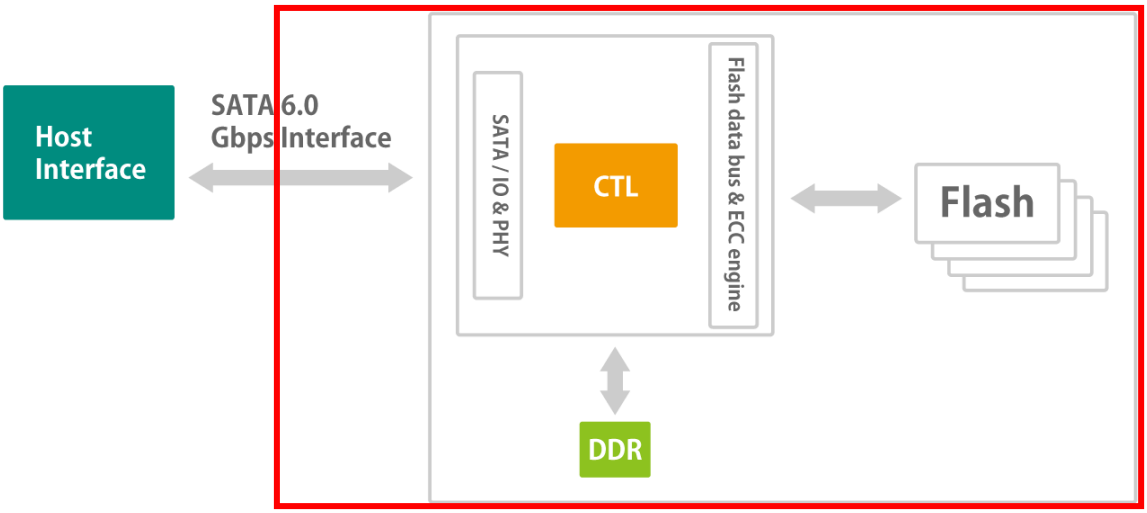

Figure 5 – Module Block Diagram

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

1.3 Modes of Operation

The Module has a single FIPS approved mode of operation (Initialized). Configuration and policy determine the Module's FIPS mode of operation. The Module enters FIPS approved mode after successful completion of the Initialize Cryptographic instructions. See "9.4 Security Initialization" for information on the Module's initialization rules. The operator can determine if the Module is operating in a FIPS approved mode by invoking the Show Status service. If the Crypto-Officer executes the Initialize Cryptographic instructions provided in "9.4 Security Initialization" with the intent of placing the Module in FIPS approved mode, the Crypto-Officer must first execute the PSID Revert service to zeroize the Module.

The PSID Revert service may be invoked as an unauthenticated service to transition the Module back to the as-manufactured state (Uninitialized). This corresponds to exiting the FIPS approved mode of operation and is akin to a "restore to factory defaults" operation. This operation also provides a means to zeroize keys and CSPs. Subsequently, the Module has to be re-initialized before it can return to a FIPS compliant mode of operation.

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

2. Cryptographic Functionality

2.1 Approved Algorithms

The Module implements the FIPS Approved cryptographic functions listed in the tables below.

Table 4 – Approved and CAVP Validated Cryptographic Functions

Validation No.	Algorithm	Algorithm Capabilities
A672	AES	Modes: CBC, CFB, ECB, CTR, OFB Direction: Decrypt, Encrypt Key Length: 128, 192, 256
	AES	Modes: XTS Direction: Decrypt, Encrypt Key Length: 128, 256
	SHA-256	Message Length: 8-51200 Increment 8
	RSA	Key Size: 2048 SigVer: PKCS1.5

2.2 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in “3.3 Services”.

Table 5 – Critical Security Parameters (CSPs)

CSP Name	Type	Description
DEK	256-bit key	To encrypt and decrypt user data: - Imported from client tool - Plaintext in flash - No output - Zeroized by command
CO Password	6-32 characters	To authenticate Crypto Officer Role: - Imported from client tool - Plaintext in flash - No output - Zeroized by command
User Password	6-32 characters	To authenticate User Role - Imported from client tool - Plaintext in flash - No output - Zeroized by command

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

2.3 Public Security Parameters

This section contains information on non-confidential security parameters such as public cryptographic keys.

Table 6 – Public Security Parameters (PSPs)

PSP Name	Type	Description
MSID	16 characters	To initialize the Module
PSID	32 characters	To call the TCG Revert service
FW_Pub	2048-bit RSA public key	To verify the signature of the firmware

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

3. Roles, Authentication and Services

3.1 Assumption of Roles

The Module supports two distinct operator roles, Crypto Officer (CO) and User. The Module enforces the separation of roles using a credential (named password or PIN) that is provisioned for the administrator (CO) and User roles as part of taking ownership and personalization of the Opal security subsystem. The credential is verified as part of authentication as the specific role during session startup to the Opal Security Subsystem. Access control over configuration mechanisms under control of the administrator is enforced by the Module firmware.

The Module does not support concurrent operators. If multiple successful authentications occur in an active session to the Opal security subsystem to multiple roles, modifications are possible to the Opal security subsystem under both roles simultaneously, however, it is assumed that the separation is performed by the human operators and not by the Module or the software that is the session owner. Neither the administrator credential nor user credential are discoverable/readable through the Opal Security Subsystem, regardless of the active authentication state in the session.

The table below lists the roles, type of authentication, authentication mechanism and associated authenticated data types supported by the Module. The Module does not support a maintenance role and/or bypass capability. The roles supported by the Module are defined in the following table.

Table 7 – Roles Description

Role ID	Authentication Data	Authentication Type	Authentication Mechanism
Crypto Officer	Password	Role-based	1. Password must be between 6 and 32 characters 2. 5 attempts are possible before requiring a power on reset of the Module 3. Probability of $1/62^6$ in a single random attempt
User	Password	Role-based	

3.2 Authentication Methods

Per the security rules and guidance, the password/PIN length must be at least 6 characters. See Rule 3 in 9.2 Operational Guidance for the Device. Password/PIN must be a combination of letters, upper- or lower-case form (A-Z, a-z) and numbers (0-9) of 6-32 characters in length. Thus, the probability of guessing a password/PIN in a single attempt is $1/62^6$. This easily meets the FIPS 140-2 authentication strength requirements of less than 1/1,000,000.

Each authentication attempt takes at least 15ms to complete and the number of attempts is limited to TryLimit, which is set to 5 in manufacturing time. This means that a theoretical maximum of {(60*1000)/15} attempts can be processed in one minute. Thus, the probability of multiple random attempts to succeed in one minute is $4000/62^6$. This is significantly lower than the FIPS requirement of 1/100,000. After 5 consecutive unsuccessful password validation attempts have occurred, the Module shall require a power cycle before any more authentication attempts are allowed.

Table 8 – Strength of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password (Min: 6 characters, Max: 32 characters) Authentication	- Probability of $1/62^6$ in a single random attempt - Probability of $4000/62^6$ in multiple random attempts in a minute

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

3.3 Services

All services implemented by the Module are listed in Table 9 and Table 10 below. Each service description also describes all usage of CSPs by the service.

Table 9 – Authenticated Services

Service	Description	CO	User
Set DEK	Input DEK manually.	V	
Set Password	Set Password which changes the operator authentication credential.	V	
Change Password	Change any password in Admin SP	V	
Setup Locking Range	Set start LBA and end LBA of the Locking Range	V	
Set Locking Range State	Set access rights of the Locking Range	V	
Lock/Unlock Locking Range	Lock/Unlock the Locking Range	V	V
List Locking Range	List all Locking Ranges	V	
Read/Write Data	Decryption/Encryption of user data		V

Table 10 – Unauthenticated Services

Service	Description
Get MSID	Get Manufactured SID, a public value that is used as default password.
PSID Revert	Destroys all CSPs and data.
Show Status	Get information about the operational state of the drive. Use TCG Level 0 Discovery
Self-test	Perform Approved Algorithm KAT and check firmware integrity.
Firmware Download	The Module allows the firmware to be updated through the ATA Download Microcode command. This authentication mechanism is used to verify the firmware using RSASSA-PKCS1-v1.5 signature verification with SHA256 and FW_Pub.

Table 11 below 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 when the Module overwrites an existing CSP.
- Z = Zeroize: The Module zeroizes the CSP.

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Table 11 – Access Rights within Services

Service	DEK	CO Password	User Password	MSID	PSID	FW_Pub
Set DEK	W					
Set Password		W	W	R		
Change Password		R/W/Z	R/W/Z			
Setup Locking Range		R				
Set Locking Range State		R				
Lock/Unlock Locking Range		R	R			
List Locking Range						
Read/Write Data	R					
Get MSID				R		
PSID Revert	Z	Z	Z		R	
Show Status						
Self-test						
Firmware Download						R

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

4. Physical Security

4.1 Apacer SV240 2.5” Form Factor Physical Security Policy

The Apacer SV240 2.5” form factor module is a multi-chip embedded device. The Module includes the following physical security mechanisms:

- The Module consists of production-grade components enclosed in an aluminum alloy enclosure, which is opaque within the visible spectrum. The physical enclosure functions as the security boundary of the Module. The only components exposed are the SATA Data and Power ports. The Module does not support a maintenance access interface. The top panel of the enclosure can be removed by unscrewing screws. However, the Module is sealed with tamper-evident labels in accordance with FIPS 140-2 Level 2 Physical Security requirements so that tampering is easily detected when the top and bottom cases are detached.

- Two (2) tamper-evident labels are applied over both top and bottom cases of the Module by Apacer during the manufacturing process. These labels cannot be removed and/or reapplied without tamper evidence. The position of the two tamper evident seals is indicated in the following image.

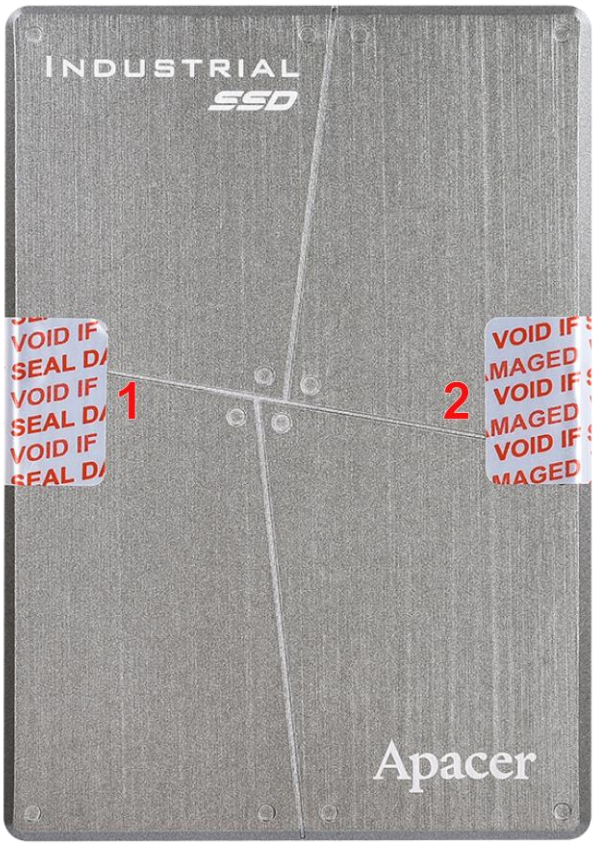

Figure 6 – Apacer SV240 2.5” Form Factor Physical Enclosure - Top

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Figure 7 – Apacer SV240 2.5” Form Factor Physical Enclosure - Side

Figure 8 – Apacer SV240 2.5” Form Factor Physical Enclosure - Bottom

The Module should be examined at regular intervals for evidence according to the following guidance. In all cases of evidence of tampering being detected, the device should be removed from service.

Table 12 – Apacer SV240 2.5” Form Factor Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Production grade cases	On initial receipt of the device and when feasible afterwards.	Inspect the entire perimeter for cracks, gouges, lack of enclosure, bent clips, and other signs of tampering.
Tamper-evident Sealing Labels		Inspect the sealing labels for scratches, gouges, cuts and other signs of tampering.

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

4.2 Apacer SV240 M.2 Form Factor Physical Security Policy

The Apacer SV240 M.2 form factor module is a multi-chip embedded device. The Module includes the following physical security mechanisms:

- The Module is surrounded by an opaque epoxy which is applied by Apacer during the manufacturing process. This coating functions as the physical security boundary of the device. The only components exposed are the SATA Data and Power ports. The Module does not support a maintenance access interface. This is illustrated in the following figures:

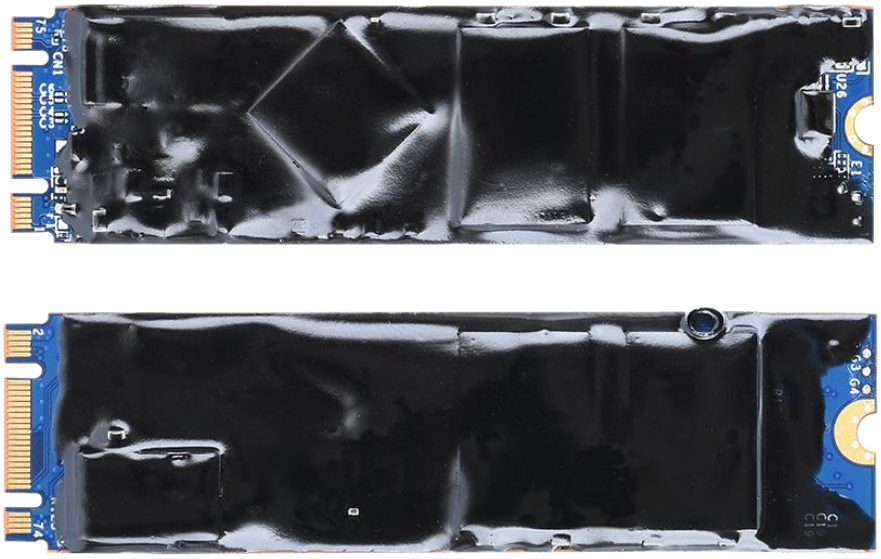

Figure 9 – Apacer SV240 M.2 Form Factor Epoxy Coating: Top and Bottom

The Module should be examined at regular intervals for evidence according to the following guidance. In all cases of evidence of tampering being detected, the device should be removed from service.

Table 13 – Apacer SV240 M.2 Form Factor Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Opaque packaging	On initial receipt of the device and when feasible afterwards.	Check packaging for attempts to remove the epoxy coating and inspect for cuts, gouges etc.

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

4.3 Apacer SV240 MO-297 Form Factor Physical Security Policy

The Apacer SV240 MO-297 form factor module is a multi-chip embedded device. The Module includes the following physical security mechanisms:

- The Module is surrounded by an opaque epoxy which is applied by Apacer during the manufacturing process. This coating functions as the physical security boundary of the device. The only components exposed are the SATA Data and Power ports. The Module does not support a maintenance access interface. This is illustrated in the following figures:

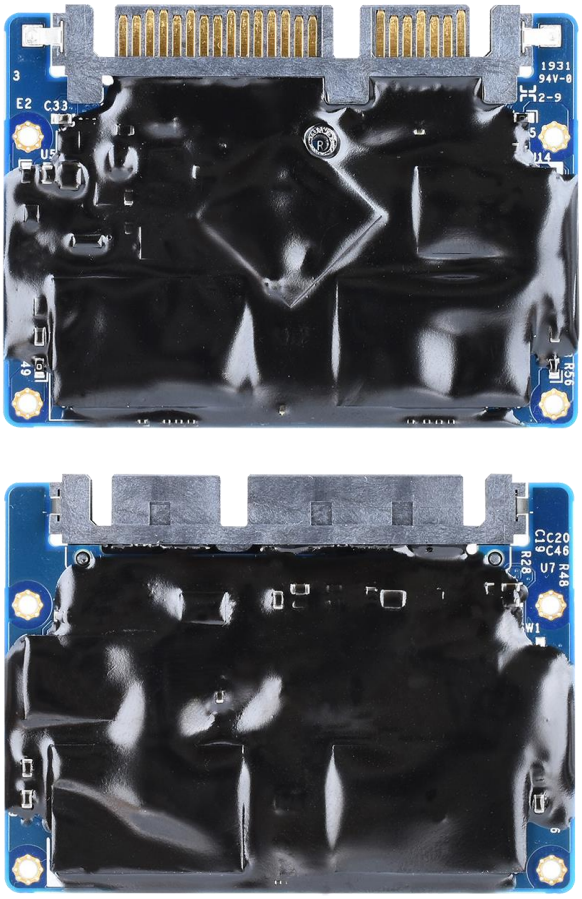

Figure 10 – Apacer SV240 MO-297 Form Factor Epoxy Coating: Top and Bottom

The Module should be examined at regular intervals for evidence according to the following guidance. In all cases of evidence of tampering being detected, the device should be removed from service.

Table 14 – Apacer SV240 MO-297 Form Factor Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Opaque packaging	On initial receipt of the device and when feasible afterwards.	Check packaging for attempts to remove the epoxy coating and inspect for cuts, gouges etc.

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

4.4 Apacer SV240 MO-300 Form Factor Physical Security Policy

The Apacer SV240 MO-300 form factor module is a multi-chip embedded device. The Module includes the following physical security mechanisms:

- The Module is surrounded by an opaque epoxy which is applied by Apacer during the manufacturing process. This coating functions as the physical security boundary of the device. The only components exposed are the SATA Data and Power ports. The Module does not support a maintenance access interface. This is illustrated in the following figures:

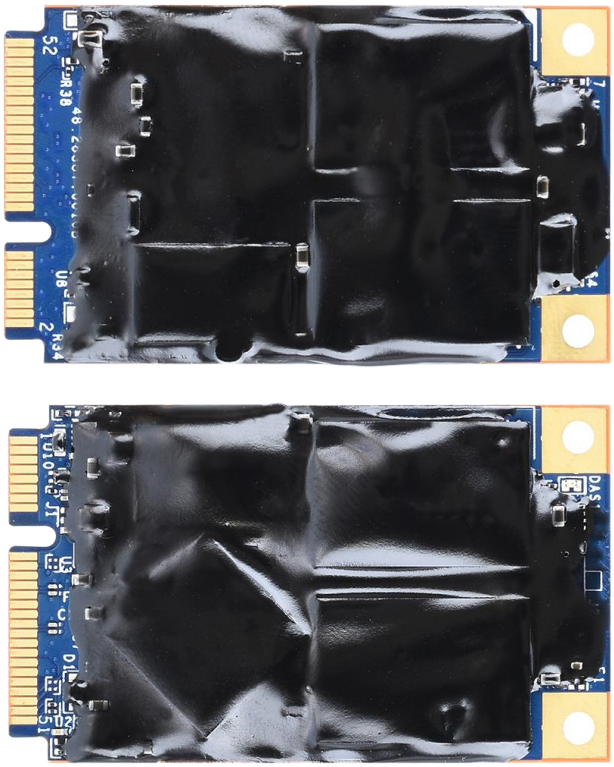

Figure 11 – Apacer SV240 MO-300 Form Factor Epoxy Coating: Top and Bottom

The Module should be examined at regular intervals for evidence according to the following guidance. In all cases of evidence of tampering being detected, the device should be removed from service.

Table 15 – Apacer SV240 MO-300 Form Factor Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Opaque packaging	On initial receipt of the device and when feasible afterwards.	Check packaging for attempts to remove the epoxy coating and inspect for cuts, gouges etc.

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

5. Operational Environment

The Module operates in a non-modifiable operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this Module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

6. Electromagnetic Interference/ Electromagnetic Compatibility (EMI/EMC)

The Module successfully completed EMI/EMC testing and conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

7. Mitigation of Other Attacks Policy

The Module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2.

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

8. Self-tests

Each time the Module is powered up, it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self-tests are available on demand by power cycling the Module.

On power up or reset, the Module performs self-tests described in Table 16 and Table 17 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters the self-test error state; if a power up self-test fails, the Module will not respond or will not enumerate.

Table 16 – Power Up Self-tests

Test Target	Description
Firmware Integrity	Firmware integrity check using 16-bit CRC
AES	Encrypt KAT and Decrypt KAT for AES Modes: ECB, XTS Key size: 256 bits
SHA	KAT for SHA-256
RSA	KAT for RSA

Table 17 – Conditional Self-tests

Test Target	When Executed	Description
Firmware Load Test	When new firmware is downloaded	Digital Signature Verification by RSA
Manual Key Entry Test	When all manually-entered keys (DEKs) are entered into the Module	EDC by 16-bit checksum

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

9. Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the Module to implement the security requirements of this FIPS 140-2 Level 2 Module.

9.1 Operational Rules for the User/Operator

1. The Module does not support concurrent operators.
2. In Opal Security State a security rule is that the host must not authenticate to more than one operator (TCG authority) in a session. To clear the authentication the session must close or the Module must be power cycled.

9.2 Operational Guidance for the Device

1. Requires the operator to be authenticated before having access to any cryptographic service other than those outlined in “3. Roles, Authentication and Services”.
2. The operator is capable of commanding the Module to perform the power up self-tests by cycling power or resetting the Module.
3. At installation set all operator PINs applicable for the Security State to private values of 6-32 characters in length. PINs must be a combination of alphanumeric characters including A-Z, a-z and 0-9.
4. The Module enforces a maximum authentication attempt before a reset is required to continue. After 5 consecutive unsuccessful password validation attempts have occurred, the Module shall require a power cycle before any more authentication attempts are allowed.

9.3 Operational Behavior of the Device

1. The Module shall provide two distinct operator roles: Cryptographic Officer and User.
2. The Module shall provide role-based authentication.
3. The Module shall clear previous authentications on power cycle.
4. When the Module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
5. Power up self-tests do not require any operator action.
6. Data output shall be inhibited during self-tests, zeroization, and error states.
7. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
8. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
9. The Module does have external input/output ports used for entry/output of data.
10. The Module does not output CSPs.

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

11. The Module does not output intermediate key values.

12. The Module does not support a bypass capability service.

13. The Module does not support the update of the logical serial number or vendor ID.

14. The Module does not permit the operator to change roles.

9.4 Security Initialization

The Module is shipped from the factory in the uninitialized state. On receipt of the Module, the CO should examine the product to ensure it has not been tampered with during shipping according to the procedures outlined in “4. Physical Security”. Upon verification that the Module has not been tampered, the user should initialize the drive into the Opal Security State. The operations to initialize the Module into the FIPS approved mode of operation are as follows:

1. On initial setup, set SID and Admin1 password with MSID.

2. Enter DEK manually.

3. Enable the locking range.

4. Set up LBA values and the state of locking range.

5. Power cycle the Module.

The CO role is responsible for configuration of other CO roles and User roles as well as enabling locking/unlocking on any of the CO or User role controlled areas (locking ranges). The User roles are responsible for enabling locking/unlocking of the assigned locking ranges as well as performing locking/unlocking of their assigned locking range. In FIPS approved mode (Initialized), both the CO and User Roles require authentication and unlock prior to allowing access to data, whereas the uninitialized mode does not. The Module will be in non-approved mode of operation if not initialized.

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

10. References and Definitions

The following standards are referred to in this Security Policy.

Table 18 – References

Abbreviation	Full Specifications Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[TCG-Opal]	Storage Work Group Storage Security Subsystem Class: Opal, Version 2.01 Final, Revision 1.00
[IG]	NIST, Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, last updated November 5, 2021
[DTR]	Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, last updated January 4, 2011
[AOUM]	Apacer Opaque User Manual, Version 1.1, March 5, 2020

Table 19 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
CO	Cryptographic Officer
CSP	Critical Security Parameters
DDR	Double Data Rate
DEK	Data Encryption Key
ECB	Electronic Code Book mode of AES encryption/decryption
KAT	Known Answer Test
MSID	Manufactured SID, Public value that is used as default password
NAND	NAND Flash Memory
POST	Power On Self-Test
PSID	Physical SID, a public unique value for each drive
PSP	Public Security Parameter
SATA	Serial Advanced Technology Attachment
SHA	Secure Hash Algorithm
SID	Secure ID
SSD	Solid State Drives
TCG	Trusted Computing Group
XTS	**X**EX **T**weakable Block Cipher with Ciphertext **S**tealing. A mode of AES.

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Revision History

Revision	Description	Date
1.0	Initial release	12/3/2021
1.1	Removed the expression of non-approved mode of operation from 9.4 Security Initialization and changed it to uninitialized state to avoid confusion	8/15/2022

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Global Presence

Taiwan (Headquarters)
Apacer Technology Inc.
1F., No.32, Zhongcheng Rd., Tucheng Dist.,
New Taipei City 236, Taiwan R.O.C.
Tel: 886-2-2267-8000
Fax: 886-2-2267-2261
amtsales@apacer.com

U.S.A.
Apacer Memory America, Inc.
46732 Lakeview Blvd., Fremont, CA 94538
Tel: 1-408-518-8699
Fax: 1-510-249-9551
sa@apacerus.com

Japan
Apacer Technology Corp.
6F, Daiyontamachi Bldg., 2-17-12, Shibaura, Minato-Ku,
Tokyo, 108-0023, Japan
Tel: 81-3-5419-2668
Fax: 81-3-5419-0018
jpservices@apacer.com

Europe
Apacer Technology B.V.
Science Park Eindhoven 5051 5692 EB Son,
The Netherlands
Tel: 31-40-267-0000
Fax: 31-40-290-0686
sales@apacer.nl

China
Apacer Electronic (Shanghai) Co., Ltd
Room D, 22/FL, No.2, Lane 600, JieyunPlaza,
Tianshan RD, Shanghai, 200051, China
Tel: 86-21-6228-9939
Fax: 86-21-6228-9936
sales@apacer.com.cn

India
Apacer Technologies Pvt Ltd,
1874, South End C Cross, 9th Block Jayanagar,
Bangalore-560069, India
Tel: 91-80-4152-9061/62
Fax: 91-80-4170-0215
sales_india@apacer.com

Apacer Technology Inc.
This document can be reproduced and distributed only whole and intact, including this copyright notice.