Phison Electronics Corporation

Phison PASCARI X and D-series NVMe TCG OPAL SSC Self-Encrypting Enterprise SSD

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for Phison PASCARI X and D-series NVMe TCG OPAL SSC Self-Encrypting Enterprise SSD, hereafter denoted the “cryptographic module”, “CM”, or “module”. The security policy describes how the cryptographic module products meet FIPS 140-3 overall Security Level 2 security requirement.

This document follows the requirements of the FIPS 140-3 (Appendix B) and NIST SP 800-140Br1 standards.
This document is non-proprietary and may be reproduced in its original entirety.

1.2 Security Levels

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	2
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Phison PASCARI X and D-series NVMe TCG OPAL SSC Self-Encrypting Enterprise SSD is a hardware module that provides user data protection while data is at rest. The cryptographic module is designed for enterprise storage solutions and to provide a wide range of cryptographic services using FIPS approved algorithms. Services include hardware-based data encryption, instantaneous user data disposal with cryptographic erase, independently controlled and protected user data LBA ranges, and authenticated FW download. The services are provided through an industry-standard TCG Opal SSC and NVMe interface.

Module Type: Hardware

Module Embodiment: Multi-Chip Embedded

Cryptographic Boundary:

The cryptographic boundary is the enclosure case. The physical interface to the cryptographic module is the PCIe connector. The logical interface includes the industry-standard NVMe and TCG Opal SSC protocols, carried on the PCIe interface.

Figure 1: Phison PASCARI-X100 and Nytro-series U.2/U.3 15mm Module Picture

Figure 2: Phison PASCARI-X100 and Nytro-series U.2/U.3 15mm for larger capacities Module Picture

Figure 3: Phison PASCARI-X100 and Nytro-series U.2 7mm Module Picture

Figure 4: Phison PASCARI-X200, X201, D205V and D206V series U.2 15mm Module Picture

Figure 5: Phison PASCARI-X200, D205V and D206V series U.2 15mm for larger capacities Module Picture

Figure 6. Phison PASCARI-X200, X201, D205V and D206V series E3.S Module Picture

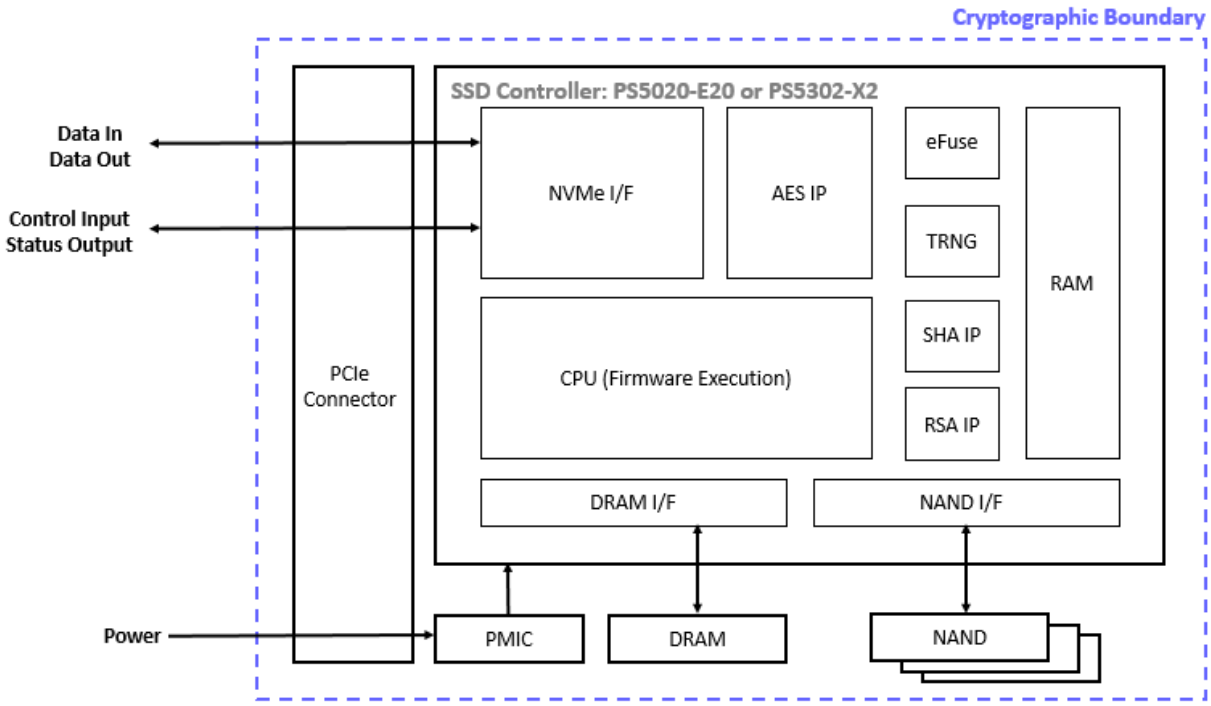

Figure 7: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Nytro 5550H 15mm U.2/U.3 Mixed Use (3 DWPD) / XP800LE70025	U.2/U.3_Single Board_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	800GB 15mm form factor high performance mixed use self-encrypting NVMe SSD
Nytro 5350H 15mm U.2/U.3 Read Intensive (1 DWPD) / XP15360SE70025	U.2/U.3_Pro_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	15360GB 15mm form factor high performance read intensive self-encrypting NVMe SSD
Nytro 5350H 15mm U.2/U.3 Read Intensive (1 DWPD) / XP1920SE70025	U.2/U.3_Single Board_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	1920GB 15mm form factor high performance read intensive self-encrypting NVMe SSD
Nytro 5350H 15mm U.2/U.3 Read Intensive (1 DWPD) / XP3840SE70025	U.2/U.3_Single Board_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	3840GB 15mm form factor high performance read intensive self-encrypting NVMe SSD
Nytro 5350H 15mm U.2/U.3 Read Intensive (1 DWPD) / XP7680SE70025	U.2/U.3_Single Board_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	7680GB 15mm form factor high performance read intensive self-encrypting NVMe SSD
Nytro 5350M 15mm U.2/U.3 Read	U.2/U.3_Pro_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	15360GB 15mm form factor

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Intensive (1 DWPD)/ XP15360SE70055				mainstream performance read intensive self-encrypting NVMe SSD.
Nytro 5350M 15mm U.2/U.3 Read Intensive (1 DWPD)/ XP1920SE70055	U.2/U.3_Single Board_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	1920GB 15mm form factor mainstream performance read intensive self-encrypting NVMe SSD.
Nytro 5350M 15mm U.2/U.3 Read Intensive (1 DWPD)/ XP3840SE70055	U.2/U.3_Single Board_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	3840GB 15mm form factor mainstream performance read intensive self-encrypting NVMe SSD.
Nytro 5350M 15mm U.2/U.3 Read Intensive (1 DWPD)/ XP7680SE70055	U.2/U.3_Single Board_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	7680GB 15mm form factor mainstream performance read intensive self-encrypting NVMe SSD.
Nytro 5350M 7mm U.2/U.3 Read Intensive (1 DWPD)/ XP1920SE10025	U.2/U.3_7mm__V1.0	SE4SA550	PS5020-E20, ARM Cortex-R5	1920GB 7mm form factor mainstream performance read intensive self-encrypting NVMe SSD.
Nytro 5350M 7mm U.2/U.3 Read Intensive (1 DWPD)/ XP3840SE10025	U.2/U.3_7mm__V1.0	SE4SA550	PS5020-E20, ARM Cortex-R5	3840GB 7mm form factor mainstream performance

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
				read intensive self-encrypting NVMe SSD.
Nytro 5350M 7mm U.2/U.3 Read Intensive (1 DWPD)/ XP7680SE10025	U.2/U.3_7mm__V1.0	SE4SA550	PS5020-E20, ARM Cortex-R5	7680GB 7mm form factor mainstream performance read intensive self-encrypting NVMe SSD.
Nytro 5550H 15mm U.2/U.3 Mixed Use (3 DWPD) / XP12800LE70025	U.2/U.3_Pro_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	12800GB 15mm form factor high performance mixed use self-encrypting NVMe SSD
Nytro 5550H 15mm U.2/U.3 Mixed Use (3 DWPD) / XP3200LE70025	U.2/U.3_Single Board_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	3200GB 15mm form factor high performance mixed use self-encrypting NVMe SSD
Nytro 5550H 15mm U.2/U.3 Mixed Use (3 DWPD) / XP6400LE70025	U.2/U.3_Single Board_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	6400GB 15mm form factor high performance mixed use self-encrypting NVMe SSD
Nytro 5550H 15mm U.2/U.3 Mixed Use (3 DWPD) / XP1600LE70025	U.2/U.3_Single Board_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	1600GB 15mm form factor high performance mixed use self-encrypting NVMe SSD

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Nytro 5550M 15mm U.2/U.3 Mixed Use (3 DWPD)/ XP12800LE70055	U.2/U.3_Pro_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	12800GB 15mm form factor mainstream performance mixed use self-encrypting NVMe SSD.
Nytro 5550M 15mm U.2/U.3 Mixed Use (3 DWPD)/ XP1600LE70055	U.2/U.3_Single Board_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	1600GB 15mm form factor mainstream performance mixed use self-encrypting NVMe SSD.
Nytro 5550M 15mm U.2/U.3 Mixed Use (3 DWPD)/ XP3200LE70055	U.2/U.3_Single Board_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	3200GB 15mm form factor mainstream performance mixed use self-encrypting NVMe SSD.
Nytro 5550M 15mm U.2/U.3 Mixed Use (3 DWPD)/ XP6400LE70055	U.2/U.3_Single Board_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	6400GB 15mm form factor mainstream performance mixed use self-encrypting NVMe SSD
Nytro 5550M 15mm U.2/U.3 Mixed Use (3 DWPD)/ XP800LE70055	U.2/U.3_Single Board_V1.0	SE4SA550 SGEBHG06	PS5020-E20, ARM Cortex-R5	800GB 15mm form factor mainstream performance mixed use self-encrypting NVMe SSD

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Nytro 5550M 7mm U.2/U.3 Mixed Use (3 DWPD)/ XP1600LE10025	U.2/U.3_7mm__V1.0	SE4SA550	PS5020-E20, ARM Cortex-R5	1600GB 7mm form factor mainstream performance mixed use self-encrypting NVMe SSD
Nytro 5550M 7mm U.2/U.3 Mixed Use (3 DWPD)/ XP3200LE10025	U.2/U.3_7mm__V1.0	SE4SA550	PS5020-E20, ARM Cortex-R5	3200GB 7mm form factor mainstream performance mixed use self-encrypting NVMe SSD
Nytro 5550M 7mm U.2/U.3 Mixed Use (3 DWPD)/ XP6400LE10025	U.2/U.3_7mm__V1.0	SE4SA550	PS5020-E20, ARM Cortex-R5	6400GB 7mm form factor mainstream performance mixed use self-encrypting NVMe SSD
Nytro 5550M 7mm U.2/U.3 Mixed Use (3 DWPD)/ XP800LE10025	U.2/U.3_7mm_V1.0	SE4SA550	PS5020-E20, ARM Cortex-R5	800GB 7mm form factor mainstream performance mixed use self-encrypting NVMe SSD
PASCARI D205V Series E3.S/ DP20KK0C-F-32T7	D205V_E3.S_V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	32TB, E3.S form factor
PASCARI D205V Series E3.S/ DP20KK0D-F-32T7	D205V_E3.S_V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	32TB, E3.S form factor
PASCARI D205V Series E3.S/ DP20KK0D-F-65T5	D205V_E3.S_V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	64TB, E3.S form factor
PASCARI D205V Series E3.S/ DX20KK0C-F-32T7	D205V_E3.S_V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	32TB, E3.S form factor

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
PASCARI D205V Series E3.S/ DX20KK0D-F-32T7	D205V_E3.S_V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	32TB, E3.S form factor
PASCARI D205V Series E3.S/ DX20KK0D-F-65T5	D205V_E3.S_V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	64TB, E3.S form factor
PASCARI D205V Series U.2 15mm/ DP20JK0C-F-16T3	D205V_U.2_ single board _V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	16TB, 15mm U.2 form factor
PASCARI D205V Series U.2 15mm/ DP20JK0C-F-32T7	D205V_U.2_ single board _V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	32TB, 15mm U.2 form factor
PASCARI D205V Series U.2 15mm/ DP20JK0C-F-65T5	D205V_U.2_pro_V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	64TB, 15mm U.2 form factor
PASCARI D205V Series U.2 15mm/ DP20JK0D-F-131T	D205V_U.2_pro_V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	128TB, 15mm U.2 form factor
PASCARI D205V Series U.2 15mm/ DP20JK0D-F-32T7	D205V_U.2_ single board _V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	32TB, 15mm U.2 form factor
PASCARI D205V Series U.2 15mm/ DP20JK0D-F-65T5	D205V_U.2_ single board _V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	64TB, 15mm U.2 form factor
PASCARI D205V Series U.2 15mm/ DX20JK0C-F-16T3	D205V_U.2_ single board _V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	16TB, 15mm U.2 form factor
PASCARI D205V Series U.2 15mm/ DX20JK0C-F-32T7	D205V_U.2_ single board _V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	32TB, 15mm U.2 form factor
PASCARI D205V Series U.2 15mm/ DX20JK0C-F-65T5	D205V_U.2_pro_V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	64TB, 15mm U.2 form factor
PASCARI D205V Series U.2 15mm/ DX20JK0D-F-131T	D205V_U.2_pro_V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	128TB, 15mm U.2 form factor
PASCARI D205V Series U.2 15mm/ DX20JK0D-F-32T7	D205V_U.2_ single board _V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	32TB, 15mm U.2 form factor
PASCARI D205V Series U.2 15mm/ DX20JK0D-F-65T5	D205V_U.2_ single board _V1.0	X2PM5700	PS5302-X2, ARM Cortex-R5	64TB, 15mm U.2 form factor
PASCARI D205V Series U.2 15mm/ X4153PD20515TNVF	D205V_U.2_ single board _V1.0	NA00	PS5302-X2, ARM Cortex-R5	16TB, 15mm U.2 form factor

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
PASCARI D205V Series U.2 15mm/ X4156PD20530TNVF	D205V_U.2_ single board _V1.0	NA00	PS5302-X2, ARM Cortex-R5	32TB, 15mm U.2 form factor
PASCARI D206V Series E3.S/ DP20KM01-F-32T7	D206V_E3.S_V1.0	X2PM7700	PS5302-X2, ARM Cortex-R5	32TB, E3.S form factor
PASCARI D206V Series E3.S/ DP20KM01-F-65T5	D206V_E3.S_V1.0	X2PM7700	PS5302-X2, ARM Cortex-R5	64TB, E3.S form factor
PASCARI D206V Series E3.S/ DX20KM01-F-32T7	D206V_E3.S_V1.0	X2PM7700	PS5302-X2, ARM Cortex-R5	32TB, E3.S form factor
PASCARI D206V Series E3.S/ DX20KM01-F-65T5	D206V_E3.S_V1.0	X2PM7700	PS5302-X2, ARM Cortex-R5	64TB, E3.S form factor
PASCARI D206V Series U.2 15mm/ DP20JM01-F-131T	D206V_U.2_pro_V1.0	X2PM7700	PS5302-X2, ARM Cortex-R5	128TB, 15mm U.2 form factor
PASCARI D206V Series U.2 15mm/ DP20JM01-F-32T7	D206V_U.2_single board_V1.0	X2PM7700	PS5302-X2, ARM Cortex-R5	32TB, 15mm U.2 form factor
PASCARI D206V Series U.2 15mm/ DP20JM01-F-65T5	D206V_U.2_single board_V1.0	X2PM7700	PS5302-X2, ARM Cortex-R5	64TB, 15mm U.2 form factor
PASCARI D206V Series U.2 15mm/ DX20JM01-F-131T	D206V_U.2_pro_V1.0	X2PM7700	PS5302-X2, ARM Cortex-R5	128TB, 15mm U.2 form factor
PASCARI D206V Series U.2 15mm/ DX20JM01-F-32T7	D206V_U.2_single board_V1.0	X2PM7700	PS5302-X2, ARM Cortex-R5	32TB, 15mm U.2 form factor
PASCARI D206V Series U.2 15mm/ DX20JM01-F-65T5	D206V_U.2_single board_V1.0	X2PM7700	PS5302-X2, ARM Cortex-R5	64TB, 15mm U.2 form factor
PASCARI X100 Series U.2/U.3 15mm/ XP106H00-F-16T3	U.2/U.3_pro_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	16TB, 15mm U.2/U.3 form factor
PASCARI X100 Series U.2/U.3 15mm/ XP106H00-F-2T04	U.2/U.3_single board_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	2TB, 15mm U.2/U.3 form factor
PASCARI X100 Series U.2/U.3 15mm/ XP106H00-F-32T7	U.2/U.3_pro_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	32TB, 15mm U.2/U.3form factor
PASCARI X100 Series U.2/U.3 15mm/ XP106H00-F-4T09	U.2/U.3_single board_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	4TB, 15mm U.2/U.3 form factor

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
PASCARI X100 Series U.2/U.3 15mm/ XP106H00-F-8T19	U.2/U.3_single board_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	8TB, 15mm U.2/U.3 form factor
PASCARI X100 Series U.2/U.3 15mm/ XP106H001-F-16T3	U.2/U.3_pro_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	16TB, 15mm U.2/U.3 form factor
PASCARI X100 Series U.2/U.3 15mm/ XP106H01-F-2T04	U.2/U.3_single board_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	2TB, 15mm U.2/U.3 form factor
PASCARI X100 Series U.2/U.3 15mm/ XP106H01-F-32T7	U.2/U.3_pro_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	32TB, 15mm U.2/U.3 form factor
PASCARI X100 Series U.2/U.3 15mm/ XP106H01-F-4T09	U.2/U.3_single board_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	4TB, 15mm U.2/U.3 form factor
PASCARI X100 Series U.2/U.3 15mm/ XP106H01-F-8T19	U.2/U.3_single board_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	8TB, 15mm U.2/U.3 form factor
PASCARI X100 Series U.2/U.3 15mm/ XX106H00-F-16T3	U.2/U.3_pro_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	16TB, 15mm U.2/U.3 form factor
PASCARI X100 Series U.2/U.3 15mm/ XX106H00-F-2T04	U.2/U.3_single board_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	2TB, 15mm U.2/U.3 form factor
PASCARI X100 Series U.2/U.3 15mm/ XX106H00-F-32T7	U.2/U.3_pro_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	32TB, 15mm U.2/U.3form factor
PASCARI X100 Series U.2/U.3 15mm/ XX106H00-F-4T09	U.2/U.3_single board_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	4TB, 15mm U.2/U.3 form factor
PASCARI X100 Series U.2/U.3 15mm/ XX106H00-F-8T19	U.2/U.3_single board_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	8TB, 15mm U.2/U.3 form factor
PASCARI X100 Series U.2/U.3 15mm/ XX106H01-F-16T3	U.2/U.3_pro_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	16TB, 15mm U.2/U.3 form factor
PASCARI X100 Series U.2/U.3 15mm/ XX106H01-F-2T04	U.2/U.3_single board_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	2TB, 15mm U.2/U.3 form factor
PASCARI X100 Series U.2/U.3 15mm/ XX106H01-F-32T7	U.2/U.3_pro_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	32TB, 15mm U.2/U.3 form factor
PASCARI X100 Series U.2/U.3 15mm/ XX106H01-F-4T09	U.2/U.3_single board_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	4TB, 15mm U.2/U.3 form factor

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
PASCARI X100 Series U.2/U.3 15mm/ XX106H01-F-8T19	U.2/U.3_single board_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	8TB, 15mm U.2/U.3 form factor
PASCARI X100 Series U.2/U.3 7mm / ERU3S-FA7680G-EFP	U.2/U.3_7mm_V1.0	EKPM34AE	PS5020-E20, ARM Cortex-R5	7680GB, 7mm U.2/U.3 form factor
PASCARI X200 Series E3.S/ XP20DH02-F-16T3	X2_E3.S_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	16TB, E3.S form factor
PASCARI X200 Series E3.S/ XP20DH02-F-2T04	X2_E3.S_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	2TB, E3.S form factor
PASCARI X200 Series E3.S/ XP20DH02-F-4T09	X2_E3.S_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	4TB, E3.S form factor
PASCARI X200 Series E3.S/ XP20DH02-F-8T19	X2_E3.S_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	8TB, E3.S form factor
PASCARI X200 Series E3.S/ XP20DH03-F-16T3	X2_E3.S_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	16TB, E3.S form factor
PASCARI X200 Series E3.S/ XP20DH03-F-2T04	X2_E3.S_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	2TB, E3.S form factor
PASCARI X200 Series E3.S/ XP20DH03-F-4T09	X2_E3.S_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	4TB, E3.S form factor
PASCARI X200 Series E3.S/ XP20DH03-F-8T19	X2_E3.S_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	8TB, E3.S form factor
PASCARI X200 Series E3.S/ XX20DH02-F-16T3	X2_E3.S_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	16TB, E3.S form factor
PASCARI X200 Series E3.S/ XX20DH02-F-2T04	X2_E3.S_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	2TB, E3.S form factor
PASCARI X200 Series E3.S/ XX20DH02-F-4T09	X2_E3.S_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	4TB, E3.S form factor
PASCARI X200 Series E3.S/ XX20DH02-F-8T19	X2_E3.S_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	8TB, E3.S form factor

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
PASCARI X200 Series E3.S/ XX20DH03-F-16T3	X2_E3.S_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	16TB, E3.S form factor
PASCARI X200 Series E3.S/ XX20DH03-F-2T04	X2_E3.S_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	2TB, E3.S form factor
PASCARI X200 Series E3.S/ XX20DH03-F-4T09	X2_E3.S_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	4TB, E3.S form factor
PASCARI X200 Series E3.S/ XX20DH03-F-8T19	X2_E3.S_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	8TB, E3.S form factor
PASCARI X200 Series U.2 15mm/ XP208H02-F-16T3	X2_U.2_pro_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	16TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XP208H02-F-2T04	X2_U.2_single board_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	2TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XP208H02-F-32T7	X2_U.2_pro_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	32TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XP208H02-F-4T09	X2_U.2_single board_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	4TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XP208H02-F-8T19	X2_U.2_single board_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	8TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XP208H03-F-16T3	X2_U.2_pro_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	16TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XP208H03-F-2T04	X2_U.2_single board_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	2TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XP208H03-F-32T7	X2_U.2_pro_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	32TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XP208H03-F-4T09	X2_U.2_single board_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	4TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XP208H03-F-8T19	X2_U.2_single board_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	8TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XX208H02-F-16T3	X2_U.2_pro_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	16TB, 15mm U.2 form factor

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
PASCARI X200 Series U.2 15mm/ XX208H02-F-2T04	X2_U.2_single board_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	2TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XX208H02-F-32T7	X2_U.2_pro_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	32TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XX208H02-F-4T09	X2_U.2_single board_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	4TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XX208H02-F-8T19	X2_U.2_single board_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	8TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XX208H03-F-16T3	X2_U.2_pro_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	16TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XX208H03-F-2T04	X2_U.2_single board_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	2TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XX208H03-F-32T7	X2_U.2_pro_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	32TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XX208H03-F-4T09	X2_U.2_single board_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	4TB, 15mm U.2 form factor
PASCARI X200 Series U.2 15mm/ XX208H03-F-8T19	X2_U.2_single board_V1.0	X2PM40S0	PS5302-X2, ARM Cortex-R5	8TB, 15mm U.2 form factor
PASCARI X201 Series E3.S/ XP20DH08-F-16T3	X201_E3.S_V1.0	X2PM6026	PS5302-X2, ARM Cortex-R5	16TB, E3.S form factor
PASCARI X201 Series E3.S/ XP20DH08-F-2T04	X201_E3.S_V1.0	X2PM6026	PS5302-X2, ARM Cortex-R5	2TB, E3.S form factor
PASCARI X201 Series E3.S/ XP20DH08-F-32T7	X201_E3.S_V1.1	X2PM6026	PS5302-X2, ARM Cortex-R5	32TB, E3.S form factor
PASCARI X201 Series E3.S/ XP20DH08-F-4T09	X201_E3.S_V1.0	X2PM6026	PS5302-X2, ARM Cortex-R5	4TB, E3.S form factor
PASCARI X201 Series E3.S/ XP20DH08-F-8T19	X201_E3.S_V1.0	X2PM6026	PS5302-X2, ARM Cortex-R5	8TB, E3.S form factor
PASCARI X201 Series E3.S/ XX20DH08-F-16T3	X201_E3.S_V1.0	X2PM6026	PS5302-X2, ARM Cortex-R5	16TB, E3.S form factor

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
PASCARI X201 Series E3.S/ XX20DH08-F-2T04	X201_E3.S_V1.0	X2PM6026	PS5302-X2, ARM Cortex-R5	2TB, E3.S form factor
PASCARI X201 Series E3.S/ XX20DH08-F-32T7	X201_E3.S_V1.1	X2PM6026	PS5302-X2, ARM Cortex-R5	32TB, E3.S form factor
PASCARI X201 Series E3.S/ XX20DH08-F-4T09	X201_E3.S_V1.0	X2PM6026	PS5302-X2, ARM Cortex-R5	4TB, E3.S form factor
PASCARI X201 Series E3.S/ XX20DH08-F-8T19	X201_E3.S_V1.0	X2PM6026	PS5302-X2, ARM Cortex-R5	8TB, E3.S form factor
PASCARI X201 Series U.2 15mm/ XP208H0-F-8T19	X201_U.2_single board_V1.0	X2PM6026	PS5302-X2, ARM Cortex-R5	8TB, 15mm U.2 form factor
PASCARI X201 Series U.2 15mm/ XP208H08-F-16T3	X201_U.2_single board_V1.0	X2PM6026	PS5302-X2, ARM Cortex-R5	16TB, 15mm U.2 form factor
PASCARI X201 Series U.2 15mm/ XP208H08-F-2T04	X201_U.2_single board_V1.0	X2PM6026	PS5302-X2, ARM Cortex-R5	2TB, 15mm U.2 form factor
PASCARI X201 Series U.2 15mm/ XP208H08-F-32T7	X201_U.2_single board_V1.1	X2PM6026	PS5302-X2, ARM Cortex-R5	32TB, 15mm U.2 form factor
PASCARI X201 Series U.2 15mm/ XP208H08-F-4T09	X201_U.2_single board_V1.0	X2PM6026	PS5302-X2, ARM Cortex-R5	4TB, 15mm U.2 form factor
PASCARI X201 Series U.2 15mm/ XX208H08-F-2T04	X201_U.2_single board_V1.0	X2PM6026	PS5302-X2, ARM Cortex-R5	2TB, 15mm U.2 form factor
PASCARI X201 Series U.2 15mm/ XX208H08-F-4T09	X201_U.2_single board_V1.0	X2PM6026	PS5302-X2, ARM Cortex-R5	4TB, 15mm U.2 form factor
PASCARI X201 Series U.2 15mm/XX208H08-F-16T3	X201_U.2_single board_V1.0	X2PM6026	PS5302-X2, ARM Cortex-R5	16TB, 15mm U.2 form factor
PASCARI X201 Series U.2 15mm/XX208H08-F-32T7	X201_U.2_single board_V1.1	X2PM6026	PS5302-X2, ARM Cortex-R5	32TB, 15mm U.2 form factor
PASCARI X201 Series U.2 15mm/XX208H08-F-8T19	X201_U.2_single board_V1.0	X2PM6026	PS5302-X2, ARM Cortex-R5	8TB, 15mm U.2 form factor

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

The cryptographic module does not define any excluded components within the module's boundary.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	The module is operating in approved mode operation.	Approved	TCG Level 0 Discovery: FIPS Operating Mode global module Indicator (Byte 30, Bit 0) = 1; ReadLockEnabled=True; WriteLockEnabled=True
Non-Approved Mode	The module is operating in a non-approved mode of operation	Non-Approved	TCG Level 0 Discovery: FIPS Operating Mode global module Indicator (Byte 30, Bit 0) = 1; ReadLockEnabled=False; WriteLockEnabled=False

Table 3: Modes List and Description

Approved Mode of Operation

The Module ships from the manufacturer in a Non-compliant state (also referred to as the "uninitialized state") and Approved firmware. Before the operator performs the Secure Initialization steps detailed in Section 11.1, the drive will only operate in this non-compliant state and Cryptographic Officer and user authentication are not enabled.

The CM must be placed into the Approved mode of operation by setting up (configuring) the CM per the Security Rules detailed in Section 11.1 with the Drive Owner invoking the Activate method on the LockingSP during uninitialization.

The Approved mode provides services through industry-standard NVMe commands, TCG Opal commands addressed to the TCG AdminSP, and TCG LockingSP.

In the Approved mode, the CM supports multiple users with independent access control to read, write, and erase separate data areas (LBA range). By default, there is a single “Global Range” that encompasses the entire user data area. However, the Drive Owner may choose to classify one or more user data ranges to conform to the single user feature set, as defined in the Opal SSC feature set, which can be managed exclusively by the associated user role.

In addition to the Drive Owner and User(s) roles, this mode implements a CO role (Admins) to administer the additional features. These features include:

- Enable/disable additional Users
- Create and configure multiple LBA Ranges
- Assign access control of Users to LBA Ranges
- Lock/unlock LBA Ranges
- Erase LBA Ranges using Cryptographic Erase

The CM will remain in the Approved mode of operation until either a critical failure has been detected; or any ‘Exit FIPS Mode’ services is invoked; or the “Show Status” service does not return the approved mode indicator.

An operator can switch the CM between the Approved mode of operation and the non-compliant state. To do so, he must first transition to this uninitialized state (via ‘Exit FIPS Mode’ service) which will zeroize the keys and CSPs. He must then reinitialize the CM per the Security Rules detailed in Section 11. to return to an Approved mode of operation.

The module’s Approved mode of operation is enforced through configuration. Violating these ongoing policy restrictions (detailed in Section 11.) would mean that one is no longer using the drive in an Approved mode of operation.

Mode Change Instructions and Status:

In the Approved Mode, the TCG Revert methods may be invoked by an appropriately authenticated Role to transition the CM into the uninitialized state. This corresponds to the “Exit FIPS Mode” service and is akin to a “restore to factory defaults” operation. This operation also provides a means to zeroize keys and CSPs. Subsequently, the CM has to be reinitialized before it can return to an Approved mode of operation. These Revert and Revert SP methods may be invoked by the Drive Owner, AdminSP Admins, LockingSP Admins, or an unauthenticated role using the public PSID value.
The module’s ranges can be configured between the approved and non-approved mode by setting “ReadLockEnabled” and “WriteLockEnabled” to true (for the approved mode) and false

(for the non-approved mode). SSP's in these ranges will be zeroized when these changes are applied.

Any action by the operator that doesn't follow the initialization steps listed in section 11 would keep the CM in the non-compliant state.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-KW	A3307	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38F
AES-KW	A7622	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38F
AES-XTS Testing Revision 2.0	A3307	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
AES-XTS Testing Revision 2.0	A7622	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
HMAC DRBG	A3307	Prediction Resistance - No Mode - SHA2-256	SP 800-90A Rev. 1
HMAC DRBG	A7622	Prediction Resistance - No Mode - SHA2-256	SP 800-90A Rev. 1
HMAC-SHA2-256	A3307	Key Length - Key Length: 64-256 Increment 64	FIPS 198-1
HMAC-SHA2-256	A7622	Key Length - Key Length: 64-256 Increment 8	FIPS 198-1
PBKDF	A3307	Iteration Count - Iteration Count: 1-1000 Increment 1 Password Length - Password Length: 8-32	SP 800-132
PBKDF	A7622	Iteration Count - Iteration Count: 1-1000 Increment 1 Password Length - Password Length: 8-32 Increment 1	SP 800-132
RSA SigVer (FIPS186-5)	A3307	Hash Pair - Hash Algorithm - SHA2-512 Salt Length - 64 Mask Function - mgf1 Modulo - 4096 Signature Type - pss Fixed Public Exponent - 010001 Public Exponent Mode - fixed	FIPS 186-5
RSA SigVer (FIPS186-5)	A3308	Modulo - 4096 Signature Type - pss	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
RSA SigVer (FIPS186-5)	A7622	Modulo - 4096 Signature Type - pss	FIPS 186-5
RSA SigVer (FIPS186-5)	A7675	Hash Pair - Hash Algorithm - SHA2-512 Salt Length - 64 Mask Function - mgf1 Modulo - 4096 Signature Type - pss Fixed Public Exponent - 010001 Public Exponent Mode - fixed	FIPS 186-5
SHA2-256	A3307	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-256	A7622	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A3307	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-512	A3308	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-512	A7622	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A7675	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

Note: Only the algorithms specified in the table above are approved algorithms supported by the module in approved mode of operation.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric	N/A	Unmodified output from SP 800-90Ar1 DRBG and Section 4 option#1 of SP800-133r2
CKG-XTS	Key Type:Symmetric	N/A	SP 800-133r2 Section 6.3 Method 1 for use in AES XTS.

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

Name	Caveat	Use and Function
AES-XTS-256 (no security claimed)	IG 2.4.A Scenario 2	TCG Table obfuscation
HMAC-SHA2-256 (no security claimed)	IG 2.4.A Scenario 2	TCG Table checksum

Table 6: Non-Approved, Allowed Algorithms with No Security Claimed

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
AES-KW-256 (Non-Approved)	Encrypts Key Parameter in non-approved mode
AES-XTS-256 (Non-Approved)	Encrypts User Data in non-approved mode

Table 7: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Block Cipher	BC-UnAuth	Encryption/decryption used for user data protection		AES-XTS Testing Revision 2.0: (A3307, A7622) Key Size: 256 bits Key Strength: 256 bits
Cryptographic Key Generation	CKG	The unmodified output from the SP800-90Ar1 DRBG for the creation of cryptographic keys		CKG: () Key Type: Symmetric CKG-XTS: () Key Type: Symmetric HMAC DRBG: (A3307, A7622) HMAC-SHA2-256: (A3307, A7622) SHA2-256: (A3307, A7622)
Firmware Load Check	DigSig-SigVer	Firmware load check when attempting to load new firmware onto the module		RSA SigVer (FIPS186-5): (A3307) Signature Type

Name	Type	Description	Properties	Algorithms
				: PKCSPSS Modulo : 4096 Key Strength : 152 bits RSA SigVer (FIPS186-5): (A7622) Signature Type: PKCSPSS Modulo : 4096 Key Strength : 152 bits SHA2-512: (A3307, A7622) Key Strength: 512 bits
Firmware Secure Check	DigSig-SigVer	Firmware secure check when the module is powered on.		RSA SigVer (FIPS186-5): (A3308) Signature Type: PKCSPSS Modulo: 4096 Key Strength: 152 bits SHA2-512: (A3308) Key Strength: 512 bits RSA SigVer (FIPS186-5): (A7675) Signature Type : PKCSPSS Modulo : 4096 Key Strength: 152 bits SHA2-512: (A7675) Key Strength : 512 bits
Key Derivation for Storage Application	PBKDF	Used to store encrypted keys in Flash memory		PBKDF: (A3307, A7622) HMAC-SHA2-

Name	Type	Description	Properties	Algorithms
				256: (A3307) SHA2-256: (A3307, A7622)
Key Wrapping	BC-Auth	Used for stored key wrapping		AES-KW: (A3307, A7622) Key Length: 256 bits
TCG Table Handling (No Security Claimed)	BC-UnAuth MAC	Applies obfuscation and checksum to the TCG tables	IG 2.4.A:No Security Claimed	AES-XTS (no security claimed): () HMAC-SHA2-256 (no security claimed): ()

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

PBKDF2
The module supports symmetric key derivation from a password by using PBKDF2 algorithm option 2a in IG D.N and SP800-132 with default 1000 iteration count, 256-bit Salt and HMAC-SHA2-256 while in approved mode of operation.

The password includes any value from a minimum 8 bytes to maximum 32 bytes, which leads to the probability that a random attempt correctly guesses an 8-byte password is equal to $1/(2^{64})$, and the probability that a random attempt correctly guesses a 32-byte password is equal to $1/(2^{256})$.

The derived key (PBKDF Password Key) is used to wrap the TEK in storage. The TEK is used to key-wrap with the Key Encryption Key (KEK), which in turn wraps the Data Encryption Key (DEK). These SSP's are only used in data storage applications.

AES-XTS:
The module checks to ensure Key 1 =/= Key 2 before using the keys in the XTS-AES algorithm. This check occurs within the module boundary.

2.8 RBG and Entropy

Cert Number	Vendor Name
E140	Phison

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Phison NOISEGEN T12FFC TRNG	Physical	Phison PS5020-E20, Phison PS5302-X2	1 bit	0.594772 bits	N/A

Table 10: Entropy Sources

The module collects 646 bits from the entropy source, resulting in 384 bits of security per DRBG Seed.

2.9 Key Generation

The cryptographic module performs Cryptographic Key Generation (CKG) as per SP 800-133r2 section 4 option #1. The resulting generated symmetric keys are the unmodified output from SP 800-90Ar1 DRBG.

2.10 Key Establishment

N/A for this module.

2.11 Industry Protocols

N/A for this module.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
PCIe Connector	Data Input Data Output	NVMe Command Payload
PCIe Connector	Control Input	NVMe Command Information
PCIe Connector	Status Output	NVMe Command Status
PCIe Connector	Power	Provides power to the module
LED (E3.S variant only)	Status Output	Signals to indicate the module's LED status

Table 11: Ports and Interfaces

The module does not contain a control output interface.

4 Roles, Services, and Authentication

The CM supports both Crypto Officer (CO) and User roles.

The user data read/write service the CM includes a lock-based authentication method which is described in IG 4.1.A. The model remains secure since the purpose of these services is to protect data-at-rest. The CM re-locks this unlocked service when power cycled.

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
PIN/Password Authentication	The PIN/Password has a minimum length of 8 bytes and a maximum length of 32 bytes.	Unique ID PIN/Password	8-byte PIN : 64 bits Min strength: 1/(2^64)	Try Limit=100 Probability (single attempt): 100/(2^64)

Table 12: Authentication Methods

Operator authentication is role-based. For example, the Drive Owner role has its own unique ID and PIN.

Phison establishes the authentication objectives of the module as 1/1,000,000 per single authentication attempt and 1/100,000 per minute. The module meets these objectives.

The probability that a random attempt will succeed, or a false acceptance will occur is 1/ (2^64) which is less than 1/1,000,000. The module implements a retry attribute (“TryLimit”) where after 100 unsuccessful attempts authentication is blocked until a module reset. The probability of successfully authenticating to the module within one minute is 100/ (2^64), which is still less than 1/100,000.

Note: The initial value for SID is a manufactured value (MSID). The Security Rules (Section 11) for the CM requires that the PIN values must be “personalized” to private values using the “Set PIN” service.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Drive Owner (SID)	Role	Crypto Officer	PIN/Password Authentication
LockingSP Admins	Role	Crypto Officer	PIN/Password Authentication

Name	Type	Operator Type	Authentication Methods
AdminSP Admins	Role	Crypto Officer	PIN/Password Authentication
User	Role	User	PIN/Password Authentication

Table 13: Roles

Note: Changing from any roles to crypto officer requires separate authentication.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Activate Opal	Enable CM's Opal Setting	TCG level0 return code	TCG Activate()	None	Cryptographic Key Generation Firmware Secure Check Key Derivation for Storage Application Key Wrapping TCG Table Handling (No Security Claimed)	Drive Owner (SID) - DRBG Internal State V : G,E,Z - DRBG Key: G,E,Z - KEK: G,E - Locking SP Admin Password: E - PBKDF password key: G,E - SID: W,E - TEK: G,E - User Password: E LockingSP Admins - DRBG Internal State V : G,E,Z - DRBG Key: G,E,Z - KEK: G,E - Locking SP Admin Password: E - PBKDF password

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						key: G,E - TEK: G,E - User Password: E
Authentication	Authenticate the module	TCG status code	Password / PIN	None	Key Derivation for Storage Application Key Wrapping TCG Table Handling (No Security Claimed)	AdminSP Admins - AdminSP Admin Password: W,E - KEK: E - PBKDF password key: G,E - TEK: E Drive Owner (SID) - SID: W,E LockingSP Admins - KEK: E - Locking SP Admin Password: W,E - PBKDF password key: G,E - TEK: E User - KEK: E - PBKDF password key: G,E - TEK: E - User Password: W,E
Cryptographic Erase	This service can either: 1. Erase user data in a Single User Data Range or	Zeroize Locking Range Key TCG return Status	TCG GenKey(); TCG Erase()	None	Cryptographic Key Generation TCG Table Handling (No	LockingSP Admins - AdminSP Admin Password: Z - DEK: G,Z - DRBG Internal

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	2. Erase user data in a non-Single User Data Range				Security Claimed)	State V : G,E,Z - DRBG Key: G,E,Z - KEK: E,Z - Locking SP Admin Password: Z - PBKDF password key: G,E - SID: Z - TEK: E,Z - User Password: Z User - AdminSP Admin Password: Z - DEK: G,Z - DRBG Internal State V : G,E,Z - DRBG Key: G,E,Z - KEK: E,Z - Locking SP Admin Password: Z - PBKDF password key: G,E - SID: Z - TEK: E,Z - User Password: Z
Enable / Disable AdminSP Admin	Enable / Disable an Admin SP Admin.	Allow AdminSP Admin(s) StartSession or not	TCG Set()	None	TCG Table Handling (No Security Claimed)	Drive Owner (SID)
Enable / Disable LockingSP Admin(s),	Enable / Disable a Locking SP Admin	Allow LockingSP Admin(s),	TCG Set()	None	Key Wrapping TCG Table Handling	LockingSP Admins - KEK: E - TEK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
non-SUDR User(s)	or non-SUDR User Authority	non-SUDR User(s) StartSession or not			(No Security Claimed)	
Exit FIPS Mode	Exit TCG Opal Security Mode. Note: CM will destroy user data and enter uninitialized state.	FIPS Operating Mode Indicator (Byte 30, Bit 0) = 0	TCG Revert(); TCG RevertSP()	None	Cryptographic Key Generation TCG Table Handling (No Security Claimed)	AdminSP Admins - AdminSP Admin Password: Z - DEK: G,Z - DRBG Entropy Input String: G,E,Z - DRBG Internal State V : G,E,Z - DRBG Key: G,E,Z - DRBG Seed: G,E,Z - KEK: Z - Locking SP Admin Password: Z - SID: Z - TEK: Z - User Password: Z Drive Owner (SID) - AdminSP Admin Password: Z - DEK: G,Z - DRBG Entropy Input String: G,E,Z - DRBG Internal State V : G,E,Z - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: G,E,Z - DRBG Seed: G,E,Z - KEK: Z - Locking SP Admin Password: Z - SID: Z - TEK: Z - User Password: Z LockingSP Admins - AdminSP Admin Password: Z - DEK: G,Z - DRBG Entropy Input String: G,E,Z - DRBG Internal State V : G,E,Z - DRBG Key: G,E,Z - DRBG Seed: G,E,Z - KEK: Z - Locking SP Admin Password: Z - SID: Z - TEK: Z - User Password: Z Unauthenticated - AdminSP Admin Password: Z - DEK: G,Z - DRBG Entropy Input String:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,E,Z - DRBG Internal State V : G,E,Z - DRBG Key: G,E,Z - DRBG Seed: G,E,Z - KEK: Z - Locking SP Admin Password: Z - SID: Z - TEK: Z - User Password: Z
FIPS140 Compliance Descriptor (Show Version)	Report FIPS 140 revision, overall security level, HW and FW revisions, and module name	None	Security Receive (SP = 0h, SPSP= 02h)	FIPS 140 Compliance Descriptor table data	None	Unauthenticated
Firmware Download	Load firmware image. If the self-test of the code load passes, then the device runs with the new code	NVMe Status	NVMe Firmware Commit	None	Firmware Load Check TCG Table Handling (No Security Claimed)	Drive Owner (SID) - RSA Public Key: E
Generate Random Number	Provide the random number from the module	TCG Return Status	TCG Random()	Random value	Cryptographic Key Generation	Unauthenticated - DRBG Entropy Input String: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Internal State V : G,E,Z - DRBG Key: G,E,Z - DRBG Seed: G,E,Z
Lock / Unlock FW Download	Enable / Disable FW Download Service	Unlock : allow Firmware Download Lock : Not allow Firmware Download TCG return Status	TCG Set()	None	TCG Table Handling (No Security Claimed)	Drive Owner (SID)
Lock / Unlock User Data Range for Read and/or Write	Block or allow read (decrypt) / write (encrypt) of user data in a range	Locking Range Read/Write Lock change TCG Return Status	TCG Set()	None	TCG Table Handling (No Security Claimed)	LockingSP Admins User
Reset Module (Self-Tests)	Power cycles the module, zeroizes the SSPs in RAM and runs the Self-Tests	None	POR	None	Firmware Secure Check	Unauthenticated - DRBG Entropy Input String: G,E,Z - DRBG Internal State V : G,E,Z - DRBG Key: G,E,Z - DRBG Seed: G,E,Z
Set Pin	Change operator authentication data.	TCG Return Status	TCG Set(); New password	None	Key Derivation for Storage Application	AdminSP Admins - AdminSP Admin Password:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Key Wrapping TCG Table Handling (No Security Claimed)	W,E - PBKDF password key: G,E Drive Owner (SID) - PBKDF password key: G,E - SID: W,E LockingSP Admins - Locking SP Admin Password: W,E - PBKDF password key: G,E - TEK: E - User Password: W,E User - PBKDF password key: G,E - TEK: E - User Password: W,E
Set Range Attributes for non-SUDR	Set the location, size, locking and User access rights of the non-SUDR.	Locking Range attributes change TCG Return Status	TCG Set()	None	Key Wrapping TCG Table Handling (No Security Claimed)	LockingSP Admins - KEK: E - TEK: E
Set Range Geometry for SUDR	Set the location and size of the SUDR	Locking Range geometry change TCG	TCG Set()	None	TCG Table Handling (No Security Claimed)	LockingSP Admins User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		Return Status				
Show Status	Report if the CM is either operating in the approved mode, non-approved mode or the Non-Compliant state.	Approved mode: Level 0 Device Discovery Indicator (Byte 30, Bit 0) = 1	TCG Level0Discovery()	TCG Return Status	TCG Table Handling (No Security Claimed)	Unauthenticated
User Configuration Management	Enable / Disable Single User Data Range (SUDR) classification for a data range or disable a non-SUDR user's ability to change Password.	TCG Return Status	TCG Set()	None	Key Wrapping TCG Table Handling (No Security Claimed)	LockingSP Admins - DEK: E - KEK: E - TEK: E
User Data Read/Write	Encryption / decryption of user data to/from a LBA range. Access control to this service is provided through Lock /	NVMe IO Read / Write Commands Host got LBA data from device/ Host send LBA data to device	NVMe IO Read/Write Commands	None	Block Cipher	Unauthenticated - DEK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Unlock User Data Range					

Table 14: Approved Services

Single User Data Ranges (SUDRs)
While invoking the Activate method to enter the Approved Mode, the Drive Owner may elect to classify one or more user data ranges as “Single User Data Ranges” (SUDRs). Such SUDRs conform to the Single User feature set as defined in the Opal SSC feature set and are managed solely by the associated User role. Details of the differences between SUDRs and normal data ranges are in Table 14.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Block Cipher	Encryption/decryption used for user data protection	AES-XTS-256 (Non-Approved)	Unauthenticated
Key Wrapping	Used for key wrapping	AES-KW-256 (Non-Approved)	Unauthenticated
User Data Read Write (Non-Approved)	Provides user data encryption/decryption on a non-approved range	AES-XTS-256 (Non-Approved) AES-KW-256 (Non-Approved)	Unauthenticated

Table 15: Non-Approved Services

Note: SSPs generated in the approved mode cannot be used in the non-approved mode, and vice versa

4.5 External Software/Firmware Loaded

FW can be upgraded (replaced) with a signed FW download operation. If the code download is successfully authenticated, then the module will begin operating with the new code image.

When loading a new firmware, the module performs a Firmware Load Check using RSA 4096 with SHA2-512 (Cert. #A3307) for the new validated firmware to be uploaded into the module.

5 Software/Firmware Security

5.1 Integrity Techniques

The module performs the Firmware Integrity test by using RSA Signature Verification (Cert. # A3308 and A7675) during the firmware integrity Self-Test. The firmware integrity test is run on the entire binary (.bin file) that makes up the module's firmware.

5.2 Initiate on Demand

The operator can initiate the Firmware Integrity test by power cycling the Module. Upon Module power-on, the Firmware Integrity test and the rest of the CASTs will be executed.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied:

The module will only accept firmware that has been signed with the private key associated with the Firmware Load public key that is already present within the module.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Production grade cases	The frequency of the physical inspection should be determined by the Crypto Officer. It is recommended that the enclosure be inspected monthly.	Periodic inspection to detect evidence of tampering: * Check enclosure for physical damage * Check for missing or loose screws If tampering is detected, remove the module from service. per the "End of Life" section of this document.
Two tamper-evident security labels	The frequency of the physical inspection should be determined by the Crypto Officer. It is recommended that the TEL be inspected monthly.	Periodic inspection to detect evidence of tampering: * Checkerboard pattern on TEL * Security label cutouts do not match original * Security label over PCBA screws not penetrated. If tampering is detected, remove the module from service. per the "End of Life" section of this document.

Table 16: Mechanisms and Actions Required

The Module has a multi-chip embedded embodiment and has the following physical security mechanisms which meet the physical security level 2:

1. The module consists of production-grade components enclosed in an alloy housing and is opaque within the visible spectrum.

2. Two tamper-evident security labels are applied over both top and bottom housing of the module at manufacturing. These labels prevent the removal of screws from the SSD housing, thereby restricting any further access or visibility to the multiple-chip embedded PCBA board inside.

3. The tamper-evident labels cannot be penetrated or removed and reapplied without tamper-evidence.

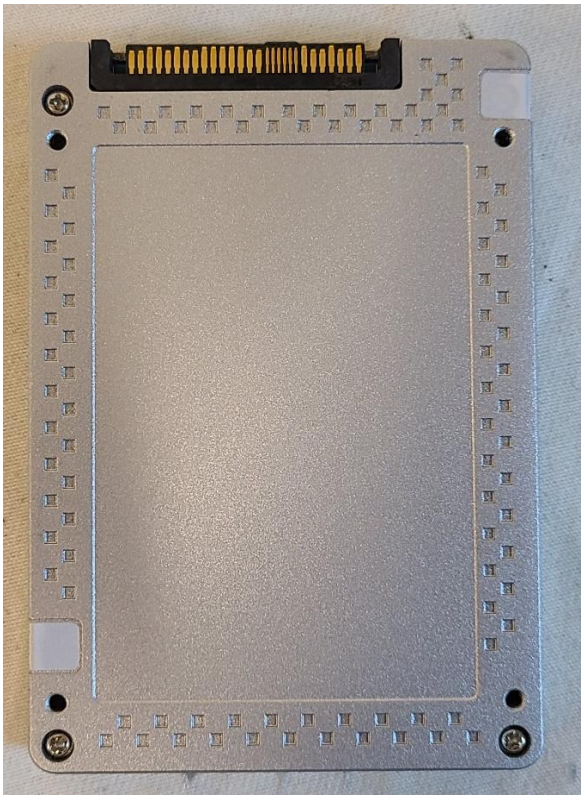

Figure 8 – Phison PASCARI-X100 series and Nytro-series U.2/U.3 15mm module Seal Application Locations

Figure 9 - Phison PASCARI-X100 series and Nytro-series U.2/U.3 15mm for larger capacities module Seal Application Locations

Figure 10 - Phison PASCARI-X100 series and Nytro-series U.2 7mm Module Seal Application Locations

Figure 11 - Phison PASCARI-X200, X201, D205V and D206V series U.2 15mm Module Picture Seal Application Location

Figure 12 - Phison PASCARI-X200,D205V and D206V series U.2 15mm for larger capacities Module Seal Application Locations

Figure 13. Phison PASCARI-X200, X201, D205V and D206V series E3.S Module Seal Application Locations

8 Non-Invasive Security

N/A for this module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Non-Volatile Memory (NAND)	SSPs are stored in encrypted form and can be deleted by certain methods.	Static
Volatile Memory (DRAM)	SSPs are stored in plaintext form and are deleted upon power-off and other specific scenarios.	Dynamic

Table 17: Storage Areas

The module stores temporary SSPs in dynamic random-access memory (RAM). Non-ephemeral SSPs are stored in NAND.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Authentication Password/PIN	Entered	Volatile Memory (RAM)	Plaintext	Manual	Electronic	

Table 18: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Cryptographic Erase	Erase user data, and zeroizes SSPs (replacing)	SSP's are immediately replaced with 0's (changing key).	Conduct the TCG Erase command (Cryptographic Erase Service)
Exit FIPS Mode	CM will enter the uninitialized state and keys and SSPs will zeroize.	This service is akin to a "Restore factory defaults" operation, and provides a means to zeroize keys and CSPs.	Available to Drive Owner, AdminSP Admin, LockingSP Admin via the TCG Revert() TCG RevertSP() commands
Reset Module	Power cycles the module, zeroizes SSP.	This service power-cycles the module, which zeroizes all SSPs in RAM due to its volatile nature.	Available without authentication by removing and applying power to the module.

Table 19: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AdminSP Admin Password	A unique value set by a certain Admin SP.	64-bit to 256-bit password - Min 64 bits, Max. 256-bits	Authentication - CSP			Key Derivation for Storage Application
DEK	LBA Range Data Encryption Keys which be used to	256 bits - 256-bits	Symmetric Key - CSP	Cryptographic Key Generation		Block Cipher

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	encrypt or decrypt the user data.					
DRBG Entropy Input String	For DRBG usage	646 bits - 384 bits	DRBG SSP - CSP	Phison NOISEGEN T12FFC TRNG		Cryptographic Key Generation
DRBG Internal State V	DRBG secret values V	256 bits - 256 bits	DRBG SSP - CSP	Cryptographic Key Generation		Cryptographic Key Generation
DRBG Key	DRBG key	256 bits - 256 bits	DRBG SSP - CSP	Cryptographic Key Generation		Cryptographic Key Generation
DRBG Seed	For DRBG usage	646 bits - 384 bits	DRBG SSP - CSP	Phison NOISEGEN T12FFC TRNG		Cryptographic Key Generation
KEK	The key to wrap the DEK	256-bits - 256-bits	Symmetric Key - CSP	Cryptographic Key Generation		Key Wrapping
Locking SP Admin Password	A unique value set by a certain Locking SP.	64-bit to 256-bit password - Min 64 bits, Max. 256-bits	Authentication - CSP			Key Derivation for Storage Application
PBKDF password key	Part of the elements that join the process to generate AES key wrap key.	256 bits - 256 bits	Encryption Key - CSP	Key Derivation for Storage Application		Key Wrapping
RSA Public Key	RSA Public Key used for firmware updated authentication.	4096 bits - 152-bits	Public Key - PSP	Preloaded		Firmware Load Check
SID	Drive Owner Pin.	64-bit to 256-bit password - Min	Authentication - CSP			Key Derivation for Storage Application

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		64 bits, Max 256-bits				
TEK	The key to wrap the KEK	256 bits - 256-bits	Symmetric Key - CSP	Cryptographic Key Generation		Key Wrapping
User Password	A unique value set by LockingSP-users.	64-bit to 256-bit password - Min 64 bits, Max. 256-bits	Authentication - CSP			Key Derivation for Storage Application

Table 20: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AdminSP Admin Password	Authentication Password/PIN	Volatile Memory (DRAM):Plaintext Non-Volatile Memory (NAND):Obfuscated	Until close session	Exit FIPS Mode Cryptographic Erase	PBKDF password key:Derives
DEK		Non-Volatile Memory (NAND):Encrypted Volatile Memory (DRAM):Plaintext	Until range relocked	Exit FIPS Mode Cryptographic Erase	KEK:Wrapped By
DRBG Entropy Input String		Volatile Memory (DRAM):Plaintext	While in Use	Exit FIPS Mode Reset Module Cryptographic Erase	DRBG Seed:Derives
DRBG Internal State V		Volatile Memory (DRAM):Plaintext	While in Use	Exit FIPS Mode Reset Module Cryptographic Erase	DRBG Seed:Derived From
DRBG Key		Volatile Memory (DRAM):Plaintext	While in Use	Exit FIPS Mode Reset Module	DRBG Seed:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Cryptographic Erase	
DRBG Seed		Volatile Memory (DRAM):Plaintext	While in Use	Exit FIPS Mode Reset Module Cryptographic Erase	DRBG Seed:Derived From DRBG Internal State V :Derives DRBG Key:Derives
KEK		Non-Volatile Memory (NAND):Encrypted Volatile Memory (DRAM):Plaintext	Until completion of service	Exit FIPS Mode Cryptographic Erase	TEK:Wrapped by DEK:Wraps
Locking SP Admin Password	Authentication Password/PIN	Volatile Memory (DRAM):Plaintext Non-Volatile Memory (NAND):Obfuscated	Until close session	Exit FIPS Mode Cryptographic Erase	PBKDF password key:Derives
PBKDF password key		Volatile Memory (DRAM):Plaintext	While in Use	Reset Module	TEK:Wraps
RSA Public Key		Volatile Memory (DRAM):Plaintext Non-Volatile Memory (NAND):Plaintext	Until completion of service	N/A	
SID	Authentication Password/PIN	Volatile Memory (DRAM):Plaintext Non-Volatile Memory (NAND):Obfuscated	Until close session	Exit FIPS Mode Cryptographic Erase	PBKDF password key:Derives
TEK		Non-Volatile Memory (NAND):Encrypted Volatile Memory (DRAM):Plaintext	Until close session	Exit FIPS Mode Cryptographic Erase	PBKDF password key:Wrapped By KEK:Wraps
User Password	Authentication Password/PIN	Volatile Memory (DRAM):Plaintext Non-Volatile Memory	Until close session	Exit FIPS Mode Cryptographic Erase	PBKDF password key:Derives

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
		(NAND):Obfuscated			

Table 21: SSP Table 2

The preceding table defines the keys / SSPs and the operators / services which use them. Note the following:

- The use of PIN SSPs for authentication is implied by the operator access control.
- All non-volatile storage of keys and SSPs is in the system area of the drive media to which there is no logical or physical access from outside of the module.
- The module uses an HMAC SP 800-90Ar1 HMAC_DRBG for key generation.
- The HMAC_DRBG is seeded by the ENT (P).

10 Self-Tests

10.1 Pre-Operational Self-Tests

Whenever the Cryptographic Module powers up, it performs cryptographic algorithm self-tests automatically before starting the execution of security functions. The pre-operational test is invoked on-demand tested by power cycling the module. All data output is inhibited while performing self-tests and depending on the self-tests that fail, the module will enter the FIPS 90B Self-Test Fail State, the ROM FIPS Self-test Fail State or FIPS Self-Test Fail State. Moreover, when the CM is in Rom FIPS Self-test state, it ceases to provide any services to the host. The error can only be cleared by power-cycling of the module.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
RSA SigVer (FIPS186-5) (A3308, A7675)	RSA 4096 with SHA-512	Signature Verification	SW/FW Integrity	Fail: Enters ROM FIPS Self-Test Fail State; Pass: proceed to the next steps	Verifies Firmware

Table 22: Pre-Operational Self-Tests

The Cryptographic Module performs the pre-operational self-test firmware integrity test utilizing the method listed above.
The RSA and SHA KATs are performed prior to the Firmware Integrity Test.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-512 (A3308, A7675)	SHA2-512	KAT	CAST	Fail: Enters ROM FIPS Self-Test Fail State	Verify	Power up
SHA2-512 (A3307, A7622)	SHA2-512	KAT	CAST	Fail: Enters FIPS Self-Test Fail State	Verify	Power up
AES-KW (A3307, A7622) Unwrap	AES Key Wrap 256-bits	KAT	CAST	Fail: Enters FIPS Self Test Fail State	Key Unwrap	Power up
AES-KW (A3307, A7622) Wrap	AES Key Wrap 256-bits	KAT	CAST	Fail: Enters FIPS Self Test Fail State	Key Wrap	Power up
AES-XTS Testing Revision 2.0 (A3307, A7622) Comparison	AES-XTS 256 bits	Nonequivalence test	Critical Function	Fail: Enters FIPS Self-Test Fail State	Verify	On XTS Key generation
AES-XTS Testing Revision 2.0 (A3307, A7622) Decrypt	AES-XTS 256 bits	KAT	CAST	Fail: Enters FIPS Self Test Fail State	Decrypt	Power up
AES-XTS Testing Revision 2.0 (A3307, A7622) Encrypt	AES-XTS 256 bits	KAT	CAST	Fail: Enters FIPS Self Test Fail State	Encrypt	Power up
ESV (E140) (APT)	Adaptive Proportion Test (APT)	Fault-Detection	CAST	Fail: Enters FIPS 90B Self-Test Fail State	Verifies that the APT threshold was not exceeded	Power up & After 1024 samples

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ESV (E140) (RCT)	Repetition Count Test (RCT)	Fault-Detection	CAST	Fail: Enters FIPS 90B Self-Test Fail State	Verifies that the RCT threshold was not exceeded	Power up & After 1024 samples
Firmware Load Check	RSA PSS signature verification of new firmware image is done before it can be loaded.	Signature Verification	SW/FW Load	Fail: Firmware Commit command Return Fail Status	Firmware Load Check	When new firmware is downloaded
HMAC DRBG Generate (A3307, A7622)	DRBG-HMAC-SHA2-256	KAT Generate Function	CAST	Fail: Enter FIPS Self Test Fail State	DRBG-HMAC-SHA2-256	Power up
HMAC DRBG Instantiate (A3307, A7622)	DRBG-HMAC-SHA2-256	KAT Instantiate Function	CAST	Fail: Enter FIPS Self Test Fail State	DRBG-HMAC-SHA2-256	Power up
HMAC DRBG Reseed (A3307, A7622)	DRBG-HMAC-SHA2-256	KAT Reseed Function	CAST	Fail: Enter FIPS Self Test Fail State	DRBG-HMAC-SHA2-256	Power up
HMAC-SHA2-256 (A3307, A7622)	HMAC-SHA2-256	KAT	CAST	Fail: Enters FIPS Self Test Fail State	Firmware HMAC	Power up
PBKDF (A3307, A7622)	PBKDF-SHA2-256	KAT	CAST	Fail: Enter FIPS Self Test Fail State	PBKDF	Power up
RSA SigVer (FIPS186-5) (A3308, A7675)	RSA PSS 4096	KAT	CAST	Fail: Enters ROM FIPS	Verify	Power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				Self-Test Fail State		
RSA SigVer (FIPS186-54) (A3307, A7622)	RSA PSS 4096	KAT	CAST	Fail: Enters FIPS Self-Test Fail State	Verify	Power up
SHA2-256 (A3307, A7622)	SHA2-256	KAT	CAST	Fail: Enters FIPS Self-Test Fail State	Verify	Power up

Table 23: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-5) (A3308, A7675)	Signature Verification	SW/FW Integrity	On Demand	Manually

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-512 (A3308, A7675)	KAT	CAST	On Demand	Manually
SHA2-512 (A3307, A7622)	KAT	CAST	On Demand	Manually
AES-KW (A3307, A7622) Unwrap	KAT	CAST	On Demand	Manually
AES-KW (A3307, A7622) Wrap	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3307, A7622) Comparison	Nonequivalence test	Critical Function	On Demand	Manually
AES-XTS Testing Revision	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
2.0 (A3307, A7622) Decrypt				
AES-XTS Testing Revision 2.0 (A3307, A7622) Encrypt	KAT	CAST	On Demand	Manually
ESV (E140) (APT)	Fault-Detection	CAST	On Demand	Manually
ESV (E140) (RCT)	Fault-Detection	CAST	On Demand	Manually
Firmware Load Check	Signature Verification	SW/FW Load	On Demand	Manually
HMAC DRBG Generate (A3307, A7622)	KAT Generate Function	CAST	On Demand	Manually
HMAC DRBG Instantiate (A3307, A7622)	KAT Instantiate Function	CAST	On Demand	Manually
HMAC DRBG Reseed (A3307, A7622)	KAT Reseed Function	CAST	On Demand	Manually
HMAC-SHA2-256 (A3307, A7622)	KAT	CAST	On Demand	Manually
PBKDF (A3307, A7622)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A3308, A7675)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-54) (A3307, A7622)	KAT	CAST	On Demand	Manually
SHA2-256 (A3307, A7622)	KAT	CAST	On Demand	Manually

Table 25: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
FIPS 90B Self-Test Fail State	APT or RCT failure leading to error state	APT or RCT failure	TCG Revert	Implicit - Module is dead and

Name	Description	Conditions	Recovery Method	Indicator
				unresponsive to host.
FIPS Self-Test Fail State	Level 0 Discovery Command payload byte 16.	Conditional Self-Test fails	Power Cycle	FIPS PASS : 080h, FIPS ERROR STATE : 0FFh
ROM FIPS Self-Test Fail State	Drive unable to boot therefore unresponsive	Pre-Operational RSA Signature Verification Firmware Integrity test is failed RSA or SHA KAT (each used in Firmware Integrity Test) fail.	Power Cycle	Implicit - Module is dead and unresponsive to host

Table 26: Error States

10.5 Operator Initiation of Self-Tests

The operator can initiate the Module's Self-Tests by power cycling the Module.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Delivery
The cryptographic module is always shipped to the Crypto Officer in sealed boxes via a commercial bonded carrier. The module is shipped from the factory with the required physical security mechanisms in place (e.g., Tamper-evident sealing labels and production grade cases).

The Crypto Officer should inspect the package for any irregular tears or openings and check the module itself for signs of tampering (e.g., scratches, tears, cracks, gouges, lack of screw(s) and other signs of tampering to ensure the module has not been compromised before initialization.

Initialization
The CM is an uninitialized state that is also considered the Non-Compliant State after manufacturing. The Cryptographic Officer (Drive Owner) needs to follow the steps below to initialize the CM in to Approved Mode of operation. The CM does not change mode across module resets. However, certain operations can result in exiting from the Approved mode. In some of these exit scenarios (e.g., POST failure), the drive cannot be restored to the Approved Mode and does not provide any FIPS services.

The following are the security rules for initialization and operation of the CM in an Approved manner.

1. Taking ownership of Opal by setting the AdminSP SID credential to something other than MSID (default password) and the private value PIN at least 8 bytes length.
2. Drive Owner executes Activate method on Locking SP
3. At installation, set all operator (Drive Owner, Admins and Users) PINs applicable for the Approved mode to private values of at least 8 bytes length
4. Set ReadLockEnabled and WriteLockEnabled to “True” on at least in one data range and it must not be modified.
5. At installation, the value of Port LockOnReset for FW Download must be set to “Power Cycle” and it must not be modified.
6. After secure initialization is complete, execute a power cycling of the module, then the module is set in an Approved mode.

At the end of these steps, the CM will be in an Approved Mode of operation. This can be verified with Show Status service with a global module Indicator (Byte 30, Bit 0) = 1.

The Crypto Officer (CO) role must examine the shipping packaging and the product packaging to ensure they have not been accessed during transit by the trusted courier. Additionally, the CO is responsible for configuring other CO and user roles, as well as enabling the locking and unlocking of CO-controlled areas (locking ranges).

User roles should regularly inspect physical security mechanisms for signs of tampering. Additionally, they are responsible for enabling and managing the locking and unlocking of their assigned locking ranges.

11.2 Administrator Guidance

The Crypto Officer oversees the initialization, configuration, and management of the module. They can receive the module from the vendor through a trusted delivery service such as DHL, UPS, or FedEx. Upon receiving the package, the Crypto Officer should inspect it for any signs of damage, such as unusual tears or openings. After opening the package, they should also check the tamper-evident seals. If any tampering is suspected, the Crypto Officer should consider the product compromised and refrain from using it.

To obtain the Administrator Guidance Manual, please contact the following personnel:
Phison: please visit: https://www.phison.com/en/contact and leaving your information in the “Get In Touch” area.

11.3 Non-Administrator Guidance

Inspect the CM for any damage to the case or PCIe connector. If users notice any damage to the SSD, they should inform the Crypto Officer immediately.

11.4 Design and Rules

Ongoing Policy Restrictions:
Prior to assuming a new role, close the current Session and start a new Session, or do a power-on reset, so that the previous authentication is cleared.

11.6 End of Life

When the CM reaches end-of-life, the Crypto Officer must zeroize all SSPs prior to discarding the CM. The Crypto Officer shall revert the CM to the factory default state by invoking the Exit FIPS Mode service.

If the above method does not work well and the operators wish to dispose of the module, it is recommended to perform destruction actions such as disintegration, pulverization, or melting, as suggested in the SP800-88 Rev.1 guidelines. Alternatively, the module can be sent to a certified media destruction company to ensure confidentiality and prevent unauthorized individuals from accessing or using the information stored on the module.

12 Mitigation of Other Attacks

The module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-3 Security Level 2.