Persistent Systems, LLC

Wave Relay® Kernel Space Crypto Module

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.5
Date: January 14, 2026

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 version 1.1 of the Persistent Systems LLC Wave Relay® Kernel Space Crypto Module. It contains the security rules under which the Module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 2 module.

1.2 Security Levels

The FIPS 140-3 security levels for the Module are as follows from Table 1:

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	2
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

FIPS validated connectivity drives mission success. This Persistent Systems LLC Wave Relay® Kernel Space Crypto Module, hereafter denoted as the "module", is a Software-Hybrid cryptographic module operating on a single-chip device that provides FIPS validated cryptographic algorithms which are used by kernel space system services & protocols (e.g. Wave Relay, IPsec, etc.)

The Wave Relay® System is a peer-to-peer wireless MANET networking solution in which there is no master node. If any device fails, the rest of the devices continue to communicate using any remaining connectivity. By eliminating master nodes, gateways, access points, and central coordinators from the design, Wave Relay® delivers high levels of fault tolerance regardless of which nodes might fail.

2.1 Description

Purpose and Use:

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated cryptography. The module is intended to be used in various products within the vendor's portfolio of solutions. Built to create powerful, secure networks anywhere, the Module is used to unite all critical data sources in real time giving you and your team the confidence to make difficult decisions in the heart of the moment.

Module Type: Software-hybrid

Module Embodiment: SingleChip

Cryptographic Boundary:

The Module is a single-chip embodiment. Figure 1 below shows a block diagram of the cryptographic boundary. The cryptographic boundary is outlined in red and defined as a combination of the software kernel library (FIPS140.ko) and the hardware crypto IP core within the NXP i.MX 6 Series SoC (System on a Chip).

The disjoint hardware component is the hardware-only cryptographic algorithms and entropy source depicted on the left side of Figure 1 under "Crypto Accelerator and Assurance Module (CAAM)". The software component is the "FIPS Kernel Module" on the right side of Figure 1, which includes the SW Crypto Functions (which may utilize PAA), as well as the FIPS Self-Test implementations and CAAM Driver.

The Module supports both hardware (Cryptographic Accelerator and Assurance Module (CAAM)) and software based cryptographic operation. The flow of information between the components and the relation between data and the Module's interfaces are depicted through arrows.

Tested Operational Environment's Physical Perimeter (TOEPP):

The TOEPP of the Module is depicted in Figure 2 below.The TOEPP is the NXP i.MX6 SOC.

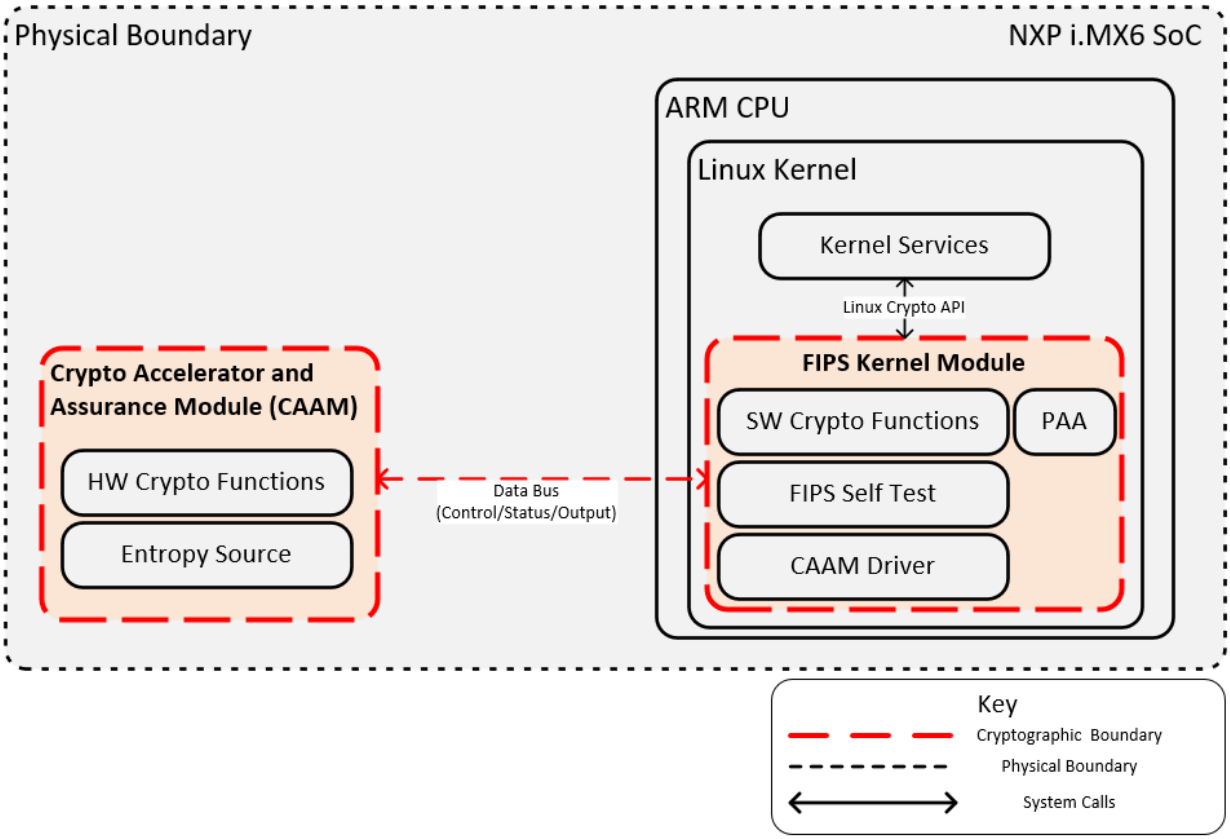
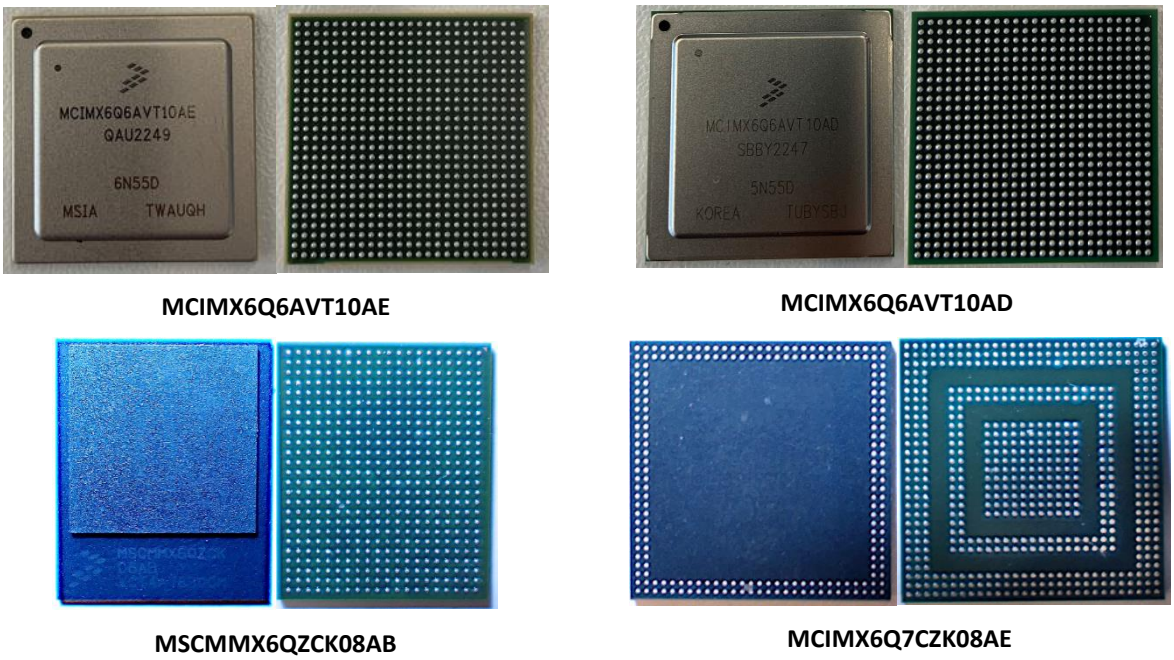


Figure 1- Cryptographic Boundary

There are four physical variants of the chip as shown in Figure 2 below.



MCIMX6Q6AVT10AE **MCIMX6Q6AVT10AD**

MSCMMX6QZCK08AB **MCIMX6Q7CZK08AE**

Figure 2 - Physical Perimeter

2.2 Tested and Vendor Affirmed Module Version and Identification

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

The cryptographic module is tested on the following operational environments:

Package or File Name	Software/ Firmware Version	Features	Integrity Test
Wave Relay	1.1		HMAC-SHA2-256

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Module Identification – Hybrid Disjoint Hardware:

The cryptographic module is tested on the following operational environments:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
MCIMX6Q6AVT10AE	MCIMX6Q6AVT10AE			
MCIMX6Q6AVT10AD	MCIMX6Q6AVT10AD			
MSCMMX6QZCK08AB	MSCMMX6QZCK08AB			
MCIMX6Q7CZK08AE	MCIMX6Q7CZK08AE			

Table 3: Tested Module Identification – Hybrid Disjoint Hardware

Tested Operational Environments - Software, Firmware, Hybrid:

Wave Relay® Kernel Space Crypto Module cryptographic module is tested on the following operational environments.

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Wave Relay® OS 2.2	MPU (5th Generation)	MCIMX6Q6AVT10AE	Yes		1.1
Wave Relay® OS 2.2	MPU (5th Generation)	MCIMX6Q6AVT10AD	Yes		1.1
Wave Relay® OS 2.2	Embedded Module	MCIMX6Q7CZK08AE	Yes		1.1
Wave Relay® OS 2.2	Embedded Module lite	MCIMX6Q7CZK08AE	Yes		1.1
Wave Relay® OS 2.2	Embedded Module	MSCMMX6QZCK08AB	Yes		1.1
Wave Relay® OS 2.2	Embedded Module lite	MSCMMX6QZCK08AB	Yes		1.1
Wave Relay® OS 2.2	GVR5	MCIMX6Q7CZK08AE	Yes		1.1
Wave Relay® OS 2.2	Integrated Antenna Series	MCIMX6Q7CZK08AE	Yes		1.1

Table 4: Tested Operational Environments - Software, Firmware, Hybrid

2.3 Excluded Components

No components were excluded from the cryptographic boundary.

2.4 Modes of Operation

Modes List and Description:

The Module supports an Approved mode and Non-Approved mode of operation. The Module does not support a degraded mode.

Mode Name	Description	Type	Status Indicator
Approved	The module supports Approved services in the Approved mode of operation. Non-Approved services are not supported in this mode.	Approved	fips140_service_indicator = 1
Non-Approved	The module is capable of non-approved services in the non-approved mode of operation only.	Non-Approved	fips140_service_indicator = 0

Table 5: Modes List and Description

Mode Change Instructions and Status:

The module provides a service level indicator. All Approved services will indicate they are Approved services and all non-Approved services will indicate they are non-Approved. No additional configuration or initialization is required.

2.5 Algorithms

Approved Algorithms:

The Module implements cryptographic algorithms in the following providers:

- Wave Relay® Kernel Space Crypto Module (HW) version 1.0 (Cert. #A4588)
- Wave Relay® Kernel Space Crypto Module (SW) version 1.0 (Cert. #A4589)

Validation certificates for each Approved security function are listed in the table below.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A4588	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A4589	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS3	A4589	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A4589	Key Length - 128, 192, 256	SP 800-38C
AES-CMAC	A4589	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A4588	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-CTR	A4589	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A4588	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A4589	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A4589	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1, 8.2.2 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A4589	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-XTS Testing Revision 2.0	A4589	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
Counter DRBG	A4589	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Hash DRBG	A4589	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A4589	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC-SHA-1	A4588	Key Length - Key Length: 8-524280 Increment 8	FIPS 198-1
HMAC-SHA-1	A4589	Key Length - Key Length: 8-524280 Increment 8	FIPS 198-1
HMAC-SHA2-224	A4588	Key Length - Key Length: 8-524280 Increment 8	FIPS 198-1
HMAC-SHA2-224	A4589	Key Length - Key Length: 8-524280 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4588	Key Length - Key Length: 8-524280 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4589	Key Length - Key Length: 8-524280 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4589	Key Length - Key Length: 8-524280 Increment 8	FIPS 198-1
HMAC-SHA2-512	A4589	Key Length - Key Length: 8-524280 Increment 8	FIPS 198-1
HMAC-SHA3-224	A4589	Key Length - Key Length: 8-524280 Increment 8	FIPS 198-1
HMAC-SHA3-256	A4589	Key Length - Key Length: 8-524280 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA3-384	A4589	Key Length - Key Length: 8-524280 Increment 8	FIPS 198-1
HMAC-SHA3-512	A4589	Key Length - Key Length: 8-524280 Increment 8	FIPS 198-1
RSA SigVer (FIPS186-4)	A4589	Signature Type - PKCS 1.5 Modulo - 2048, 3072, 4096	FIPS 186-4
SHA-1	A4588	Message Length - Message Length: 160, 0-65536 Increment 8	FIPS 180-4
SHA-1	A4589	Message Length - Message Length: 160, 0-65536 Increment 8	FIPS 180-4
SHA2-224	A4588	Message Length - Message Length: 224, 0-65536 Increment 8	FIPS 180-4
SHA2-224	A4589	Message Length - Message Length: 224, 0-65536 Increment 8	FIPS 180-4
SHA2-256	A4588	Message Length - Message Length: 256, 0-65536 Increment 8	FIPS 180-4
SHA2-256	A4589	Message Length - Message Length: 256, 0-65536 Increment 8	FIPS 180-4
SHA2-384	A4589	Message Length - Message Length: 384, 0-65536 Increment 8	FIPS 180-4
SHA2-512	A4589	Message Length - Message Length: 512, 0-65536 Increment 8	FIPS 180-4
SHA3-224	A4589	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-256	A4589	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-384	A4589	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-512	A4589	Message Length - Message Length: 0-65536 Increment 8	FIPS 202

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

The Module does not support any vendor affirmed cryptographic algorithms.

N/A for this module.

Non-Approved, Allowed Algorithms:

The module does not implement any Non-Approved, but Allowed Algorithms in the Approved Mode of Operation.

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

The module does not implement any Non-Approved, Algorithms Allowed with No Security Claimed in the Approved Mode of Operation.

N/A for this module.

Non-Approved, Not Allowed Algorithms:

The Module implements the Non-Approved, Not Allowed cryptographic algorithms listed in the table below.

Name	Use and Function
AES (GCM) - Ext IV	GCM with Externally Generated IVs
AES (GCM) - Hybrid	Hybrid Authenticated Symmetric Encryption/Decryption using internally generated IV HW: Encrypt, Decrypt SW: Message Authentication
ghash	Message Authentication used independently from AES(GCM)
AES (CCM) - Hybrid	Hybrid Authenticated Symmetric Encryption/Decryption HW: Encrypt, Decrypt SW: Message Authentication
AES (cbcmac)	Message Authentication used independently from AES(CCM)
AES (CTS)	Cipher Text Stealing
AES (XTS) - Hybrid	Hybrid Disk Encryption HW: First encryption SW: Second encryption
ENT (SW)	Software Entropy Source (Jitterentropy) for DRBG Seeding

Table 7: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

The table below shows the Security Function Implementations that the module implements:

Name	Type	Description	Properties	Algorithms
SF1	BC-Auth	Symmetric Key Data Encryption	Publication:FIPS 197	AES-CBC: (A4588, A4589) Size: 128, 192, 256 AES-CTR: (A4588, A4589) Size: 128, 192, 256 AES-ECB: (A4588, A4589) Size: 128, 192, 256 AES-CBC-CS3: (A4589) Size: 128, 192, 256 AES-CCM: (A4589) Size: 128, 192, 256 AES-GCM: (A4589) Size: 128, 192, 256 AES-XTS Testing Revision 2.0: (A4589) Size: 128, 256
SF2	BC-UnAuth	Symmetric Key Data Decryption	Publication:197	AES-CBC: (A4588, A4589) Size: 128, 192, 256 AES-CTR: (A4588, A4589) Size: 128, 192, 256 AES-ECB: (A4588, A4589) Size: 128, 192, 256

Name	Type	Description	Properties	Algorithms
				AES-CBC-CS3: (A4589) Size: 128, 192, 256 AES-CCM: (A4589) Size: 128, 192, 256 AES-GCM: (A4589) Size: 128, 192, 256 AES-XTS Testing Revision 2.0: (A4589) Size: 128, 256
SF3	MAC	Message Authentication Generation/Verification	Publication:FIPS 198, SP800-38B, SP800-38D	AES-CMAC: (A4589) AES-GMAC: (A4589) HMAC-SHA-1: (A4588, A4589) HMAC-SHA2-224: (A4588, A4589) HMAC-SHA2-256: (A4588, A4589) HMAC-SHA2-384: (A4589) HMAC-SHA2-512: (A4589) HMAC-SHA3-224: (A4589) HMAC-SHA3-256: (A4589) HMAC-SHA3-384: (A4589) HMAC-SHA3-512: (A4589)
SF4	SHA	Message Digest	Publication:FIPS 180-4, FIPS 202	SHA-1: (A4588, A4589)

Name	Type	Description	Properties	Algorithms
				SHA2-224: (A4588, A4589) SHA2-256: (A4588, A4589) SHA2-384: (A4589) SHA2-512: (A4589) SHA3-224: (A4589) SHA3-256: (A4589) SHA3-384: (A4589) SHA3-512: (A4589)
SF5	DRBG	Random Number Generation	Publication:SP800-90A	Hash DRBG: (A4589) HMAC DRBG: (A4589) Counter DRBG: (A4589)
SF6	DigSig-SigVer	Signature Verification	Publication:186-4	RSA SigVer (FIPS186-4): (A4589) Size: 2048, 3072, 4096
SF7	ENT-ESV	Entropy Generation	Publication:SP800-90B	Hash DRBG: (A4589) HMAC DRBG: (A4589) Counter DRBG: (A4589)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

Below are the documentation requirements for specific algorithms and conditions, as mandated by Implementation Guidance.

AES GCM IV Uniqueness

FIPS140-3 IG C.H, Option 2

The IV is generated internally at its entirety randomly.

The generation uses an Approved DRBG (Cert. #A4589) that is internal to the module's boundary.

The IV length is fixed at 96 bits (per SP 800-38D).

FIPS140-3 IG C.I

The XTS algorithm implementation includes a check prior to use to ensure Key_1 ≠ Key_2.

SHA-1

The use of SHA-1 by the "Hash" service is only approved for integrity checks and is not approved for use as part of a digital signature.

2.8 RBG and Entropy

Cert Number	Vendor Name
E82	persistent systems

Table 9: Entropy Certificates

The Module uses the following entropy sources:

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Wave Relay Physical Entropy Source	Physical	NXP i.MX 6	384 bits	316 bits	

Table 10: Entropy Sources

Persistent Systems is using a physical free running ring oscillator to generate entropy input for instantiation and reseed of SP 800-90A compliant DRBGs. The entropy source is the True Random Number Generator (TRNG) sub-component of an NXP i.MX 6 SoC chip. The entropy source performs all required health tests of SP 800-90B, which includes continuous, start-up and on-demand health tests. There are no configurations needed by the operator to use the entropy source in accordance with the Public Use Document for ESV Cert. #E82.

Whenever a failure is detected during the health testing, entropy data is not returned to the caller; instead, a failure code is returned to enable the caller to determine the reason for the failure. The entropy source then halts and will refuse new requests for entropy. Upon return of the failure, the operator shall reset or reboot the entropy source. The entropy source will continue to operate after being reset and passing all start-up and continuous health tests.

The default Approved DRBG used for random number generation is the HMAC_DRBG (Cert A4589) using SHA2-512.

In addition, the module also provides HMAC_DRBG, CTR_DRBG and HASH_DRBG using different mechanisms and key sizes. The DRBGs are all internally seeded by using the entropy source (ESV Cert. #E82). The security strength of the DRBG is determined by the internal mechanism selected (i.e., 256-bits security strength for a CTR_DRBG using AES-256). The operator shall select the appropriate DRBG mechanism for the security strength required when using the “Random Bit Generation” service.

2.9 Key Generation

The module does not support Key Generation Functions.

2.10 Key Establishment

Key Agreement Information

The module does not support Key Agreement Functions.

Key Transport Information

The module does not support Key Transport Functions.

2.11 Industry Protocols

The module does not implement any Industry Protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The Module's ports and associated FIPS defined logical interface categories are listed below.

Physical Port	Logical Interface(s)	Data That Passes
N/A	Control Input	o API input arguments that are used to initialize and control the operation of the module o API Commands invoking cryptographic services
N/A	Data Input	o API input arguments that provide input data for processing o Data to be encrypted, decrypted, verified, or hashed o Keys to be used in cryptographic services
N/A	Data Output	o API output arguments that return generated or processed data back to the caller o Data that has been encrypted, decrypted or verified o Hashes o Random Values generated by the module's DRBG o Random seed material for other module DRBGs
N/A	Status Output	o API call return values o Status information regarding the module
N/A	Power	N/A

Table 11: Ports and Interfaces

Note: The module does not support Control Output.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Role Based Authentication	Signature Verification	SF6	RSA 3072-bit has a security strength of 128 bits. The probability of successfully guessing the private key is 1/(2^128).	Each authentication attempt takes approximately 8.4 seconds, which results in a maximum of seven authentication attempts per minute. The probably of a brute force attack being successful within a given minute is 7/(2^128).

Table 12: Authentication Methods

4.2 Roles

The Module supports one distinct operator role, Crypto Officer (CO). One authentication is allowed per Module reset. The Module does not support concurrent operators.

The Cryptographic Officer's authentication public key is protected by the physical and logical design of the Module; it is stored as part of the Module binary itself.

The Roles Table below lists all operator roles supported by the Module.

Name	Type	Operator Type	Authentication Methods
Cryptographic Officer	Role	CO	Role Based Authentication

Table 13: Roles

4.3 Approved Services

All approved services implemented by the Module are listed in the table below:

The SSPs modes of access shown in the table below are defined as:

- G = Generate: The Module generates or derives the SSP.
- R = Read: The SSP is read from the Module (e.g., the SSP is output).
- W = Write: The SSP is updated, imported, or written to the Module (SSP is input).
- E = Execute: The Module uses the SSP in performing a cryptographic operation.
- Z = Zeroize: The Module zeroizes the SSP

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Module Self-Test	Perform module initialization, pre-operational, and conditional cryptographic algorithm self-tests.	fips_get_tests_passed()	Power	Pass/Fail Status	None	Cryptographic Officer - Software Integrity Key: E
Login	Authenticate to the module.	fips140_get_error()	Authentication Signature	Authentication Status	SF6	Cryptographic Officer - CO Authentication Key: E
Module Status	Shows module's status	fips140_get_error()	None	Status	None	Cryptographic Officer
Hash	Compute a Message Digest	fips140_service_indicator()=1	Message	Hash Value	SF4	Cryptographic Officer
Show Module Info	Shows module's versioning information	fips140_module_version()	None	Module Base Name + Module Version Number	None	Cryptographic Officer
Symmetric Encryption/Decryption	Encryption and decryption of data.	fips140_service_indicator()=1	AES Key, Plaintext or Ciphertext	Plaintext or Ciphertext	SF1 SF2	Cryptographic Officer - AES Key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Keyed MAC	Compute a Message Authentication code	fips140_service_indicator()=1	Message, HMAC or AES Key	Message Authentication Code	SF3	Cryptographic Officer - AES Key: W,E - HMAC Key: W,E
Random Bit Generation	Generates random values. Operator must select the appropriate DRBG mechanism for the security-strength desired.	fips140_service_indicator()=1	DRBG Selection	Random Values	SF5	Cryptographic Officer - CTR_DRBG-State: W,E - HMAC_DRBG-State: W,E - HASH_DRBG-State: W,E
RSA Signature Verification	Signature Verification	fips140_service_indicator()=1	RSA Public Key, Signature Message	Boolean indicating validity of signature	SF6	Cryptographic Officer - RSA Public Key: R,E
Entropy Generation	Generate entropy for internal or external DRBGs	fips140_service_indicator()=1	N/A	Entropy	SF7	Cryptographic Officer - DRBG-EI: G,R
Zeroisation	Destroys all security	fips140_get_error()=1	N/A	N/A	None	Cryptographic Officer - DRBG-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	parameters					EI: Z - CTR_DRBG-State: Z - AES Key: Z - HMAC Key: Z - RSA Public Key: Z - HMAC_DRBG-State: Z - HASH_DRBG-State: Z

Table 14: Approved Services

4.4 Non-Approved Services

All approved services implemented by the Module are listed in the table below:

Name	Description	Algorithms	Role
Authenticated Symmetric Encryption/Decryption	GCM using externally generated IVs	AES (GCM) - Ext IV	CO
Hybrid Authenticated Symmetric Encryption/Decryption	GCM or CCM encryption/decryption using a hybrid implementation in Hardware and Software	AES (GCM) - Hybrid AES (CCM) - Hybrid	CO
Hybrid Symmetric Encryption/Decryption	encryption/decryption using a hybrid implementation in Hardware and Software	AES (XTS) - Hybrid	CO
Authentication Codes	Message Authentication used independent of CCM or GCM	ghash AES (cbcmac)	CO
Entropy (SW)	Software entropy source	ENT (SW)	CO

Name	Description	Algorithms	Role
Ciphertext Stealing	AES encryption/decryption using ciphertext/stealing	AES (CTS)	CO

Table 15: Non-Approved Services

4.5 External Software/Firmware Loaded

The module does not support an External Software/Firmware Load capability.

5 Software/Firmware Security

5.1 Integrity Techniques

The Module is composed of the following component(s):

- Component 1: software cryptographic kernel library - binary
- Component 2: hardware-implemented cryptographic algorithms

The software component is protected with the authentication technique, HMAC-SHA2-256, as described in Table 16.

5.2 Initiate on Demand

The operator can initiate the integrity test on demand by power cycling the hardware.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

The Module has a modifiable operational environment under the FIPS 140-3 definitions. The tested operational environments are listed in Section 2.1.

The Operating Environment is modifiable and allows the operator to load and execute software.

How Requirements are Satisfied:

The Module supports a modifiable operational environment. The operator may load and execute software that was not included in the original evaluation as the underlying Wave Relay OS 2.2 operational environment is modifiable.

Each instance of a cryptographic module controls its own SSPs and are not owned or controlled by external processes/operators. This requirement is not enforced by administrative documentation and procedures but by the cryptographic module itself.

The operational environment provides the capability to separate individual application processes from each other in order to prevent uncontrolled access to CSPs and uncontrolled modification of SSPs

6.2 Configuration Settings and Restrictions

All cryptographic software, SPPs and control/status information is under the control of an operating system that implements mandatory access control.

The Operating system protects against unauthorized execution, unauthorized modification and unauthorized reading of SSPs and status data.

Processes that are spawned by the cryptographic module are owned by the module and are not owned by external processes/operators.

The Operating System provides an audit mechanism with the date and time of each audited event.

7 Physical Security

The design and physical security characteristics of the Wave Relay Kernel Space Crypto module meet the intent of the FIPS 140-3 Level 2 Physical Security Requirements, based on the test results described in the physical security test report.

The embodiment of the Module is a single chip, which is opaque and also provides tamper evidence. The module has been subjected to FIPS140-3 Level 2 physical security analysis.

7.1 Mechanisms and Actions Required

The module has:

- Production grade components with standard passivation (conformal coating/sealing coating) for environmental protection
- The Module has tamper-evident coating
- Susceptible to evidence of tampering on the external boundary when attempts to gain physical access
- External boundary shall be opaque to prevent knowledge of the critical areas of the module

N/A for this module.

8 Non-Invasive Security

The Module does not implement any mitigation method against non-invasive attack.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
System Memory (S1)	Stored in plaintext in volatile memory (RAM).	Dynamic
Binary (S2)	Stored in plaintext as part of the module binary itself.	Static

Table 16: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input in plaintext (IO1)	Application Software (outside)	System Memory (S1)	Plaintext	Manual	Electronic	
Output in plaintext (IO2)	System Memory (S1)	Application Software (outside)	Plaintext	Manual	Electronic	

Table 17: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Z1	Zeroisation service	Active overwriting of SSP values with 0s in volatile memory	Zeroisation service
Z2	Zeroisation upon use	Active overwriting of SSP values with 0s immediately after SSP is no longer needed.	N/A

Table 18: SSP Zeroization Methods

9.4 SSPs

All usage of these SSPs by the Module are described in the services detailed in Section 4.3

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG-EI	Entropy Input	387-771 - 128 to 256	ENT - CSP	SF7		SF5
CTR_DRBG-State	CTR_DRBG internal state (V and Key)	V is 128, Key is 128 to 256 - 128 to 256	DRBG - CSP	SF5		SF5
HMAC_DRBG-State	HMAC_DRBG internal state (V and Key)	V is 160 to 512, Key is 160 to 512 - 128 to 256	DRBG - CSP	SF5		SF5
HASH_DRBG-State	HASH_DRBG internal state (V and C)	V is 440 to 888, C is 440 to 888 - 128 to 256	DRBG - CSP	SF5		SF5
HMAC Key	Used for Message Authentication	128 to 512 - 128 to 256	MAC - CSP			SF3
AES Key	Used for encryption/decryption operations	128, 192, 256 - 128, 192, 256	Symmetric - CSP			SF1 SF2
RSA Public Key	Used for signature verification	2048, 3072, 4096 - 112,	Asymmetric - PSP			SF6

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		128, 150				
CO Authentication Key	Used for authenticating the CO	3072 - 128	Asymmetric - PSP			SF6
Software Integrity Key	Used for module integrity	256 - 256	Self-Test - Neither			SF3

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG-EI	Output in plaintext (IO2)	System Memory (S1):Plaintext	Until use completes	Z1 Z2	DRBG-State:Used to derive
CTR_DRBG-State		System Memory (S1):Plaintext	Until use completes	Z1 Z2	DRBG-EI:Derived From
HMAC_DRBG-State		System Memory (S1):Plaintext	Until use completes	Z1 Z2	DRBG-EI:Derived From
HASH_DRBG-State		System Memory (S1):Plaintext	Until use completes	Z1 Z2	DRBG-EI:Derived From
HMAC Key	Input in plaintext (IO1)	System Memory (S1):Plaintext	Until use completes	Z1 Z2	
AES Key	Input in plaintext (IO1)	System Memory (S1):Plaintext	Until use completes	Z1 Z2	
RSA Public Key	Input in plaintext (IO1)	System Memory (S1):Plaintext	Until use completes	Z1 Z2	
CO Authentication Key		Binary (S2):Plaintext	Until use completes	N/A	
Software Integrity Key		Binary (S2):Plaintext	Until use completes	N/A	

Table 20: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

The Module performs self-tests to ensure the proper operation of the Module. Per FIPS 140-3 these are categorized as either pre-operational self-tests or conditional self-tests.

Pre-operational self–tests are available on demand by power cycling the Module. The operator may invoke periodic self-tests by power cycling the module. It is recommended that periodic self-testing be performed weekly. Please note that HMAC-SHA2-256 is self-tested prior to execution of the Software Integrity Test.

The Module performs the following pre-operational self-tests in table below

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Software Integrity Test	HMAC SHA2-256	KAT	SW/FW Integrity	fips_get_tests_passed()	Executed on the kernel module.

Table 21: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

The Module performs the following conditional self-tests in the table below:

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC-Encrypt (4588)	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Encrypt	Power-On
AES-CBC-Decrypt (4588)	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Decrypt	Power-On

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CTR Encrypt (4588)	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Encrypt	Power-On
AES-CTR Decrypt (4588)	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Decrypt	Power-On
AES-ECB Encrypt (4588)	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Encrypt	Power-On
AES-ECB Decrypt (4588)	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Decrypt	Power-On
AES-CBC Encrypt (4589)	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Encrypt	Power-On
AES-CBC Decrypt (4589)	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Decrypt	Power-On
AES-CBC-CS3 Encrypt	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Encrypt	Power-On
AES-CBC-CS3 Decrypt	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Decrypt	Power-On
AES-CCM Encrypt	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Encrypt	Power-On
AES-CCM Decrypt	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Decrypt	Power-On
AES-CMAC (A4589)	Key sizes: 128, 256 bits	KAT	CAST	fips_get_tests_passed()	Generate	Power-On
AES-CTR Encrypt (4589)	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Encrypt	Power-On
AES-CTR Decrypt (4589)	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Decrypt	Power-On
AES-ECB Encrypt (4589)	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Encrypt	Power-On
AES-ECB Decrypt (4589)	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Decrypt	Power-On

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM Encrypt	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Encrypt	Power-On
AES-GCM Decrypt	Key sizes: 128, 192, 256 bits	KAT	CAST	fips_get_tests_passed()	Decrypt	Power-On
AES-XTS Encrypt	Key sizes: 128, 256 bits	KAT	CAST	fips_get_tests_passed()	Encrypt	Power-On
AES-XTS Decryt	Key sizes: 128, 256 bits	KAT	CAST	fips_get_tests_passed()	Decrypt	Power-On
Counter DRBG (A4589)	Key size: 128, 192, 256	KAT	CAST	fips_get_tests_passed()	instantiation, generate, and reseed KATs	Power-On
Hash DRBG (A4589)	SHA2-256	KAT	CAST	fips_get_tests_passed()	instantiation, generate, and reseed KATs	Power-On
HMAC DRBG (A4589)	SHA2-256, SHA2-512	KAT	CAST	fips_get_tests_passed()	instantiation, generate, and reseed KATs	Power-On
Entropy	SP800-90B Health Tests	RCT, APT	CAST	fips140_get_error()	Startup and Continuous RCT and APT per [90B] Section 4.2 and 4.4	Entropy Generation
HMAC-SHA-1 (A4588)	SHA-1	KAT	CAST	fips_get_tests_passed()	Generate	Power-On
HMAC-SHA2-224 (A4588)	SHA2-224	KAT	CAST	fips_get_tests_passed()	Generate	Power-On
HMAC-SHA2-256 (A4588)	SHA2-256	KAT	CAST	fips_get_tests_passed()	Generate	Power-On
HMAC-SHA-1 (A4589)	SHA-1	KAT	CAST	fips_get_tests_passed()	Generate	Power-On
HMAC-SHA2-224 (A4589)	SHA2-224	KAT	CAST	fips_get_tests_passed()	Generate	Power-On
HMAC-SHA2-256 (A4589)	SHA2-256	KAT	CAST	fips_get_tests_passed()	Generate	Power-On

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-384 (A4589)	SHA2-384	KAT	CAST	fips_get_tests_passed()	Generate	Power-On
HMAC-SHA2-512 (A4589)	SHA2-512	KAT	CAST	fips_get_tests_passed()	Generate	Power-On
HMAC-SHA3-224 (A4589)	SHA3-224	KAT	CAST	fips_get_tests_passed()	Generate	Power-On
HMAC-SHA3-256 (A4589)	SHA3-256	KAT	CAST	fips_get_tests_passed()	Generate	Power-On
HMAC-SHA3-384 (A4589)	SHA3-384	KAT	CAST	fips_get_tests_passed()	Generate	Power-On
HMAC-SHA3-512 (A4589)	SHA3-512	KAT	CAST	fips_get_tests_passed()	Generate	Power-On
RSA SigVer (FIPS186-4) (A4589)	Key Size: 3072-bit with SHA2-384	KAT	CAST	fips_get_tests_passed()	Signature Verification	Power-On
SHA-1 (A4588)	SHA-1	KAT	CAST	fips_get_tests_passed()	Message Digest	Power-On
SHA2-224 (A4588)	SHA2-224	KAT	CAST	fips_get_tests_passed()	Message Digest	Power-On
SHA2-256 (A4588)	SHA2-256	KAT	CAST	fips_get_tests_passed()	Message Digest	Power-On
SHA-1 (A4589)	SHA-1	KAT	CAST	fips_get_tests_passed()	Message Digest	Power-On
SHA2-224 (A4589)	SHA2-224	KAT	CAST	fips_get_tests_passed()	Message Digest	Power-On
SHA2-256 (A4589)	SHA2-256	KAT	CAST	fips_get_tests_passed()	Message Digest	Power-On
SHA2-384 (A4589)	SHA2-384	KAT	CAST	fips_get_tests_passed()	Message Digest	Power-On
SHA2-512 (A4589)	SHA2-512	KAT	CAST	fips_get_tests_passed()	Message Digest	Power-On

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA3-224 (A4589)	SHA3-224	KAT	CAST	fips_get_tests_passed()	Message Digest	Power-On
SHA3-256 (A4589)	SHA3-256	KAT	CAST	fips_get_tests_passed()	Message Digest	Power-On
SHA3-384 (A4589)	SHA3-384	KAT	CAST	fips_get_tests_passed()	Message Digest	Power-On
SHA3-512 (A4589)	SHA3-512	KAT	CAST	fips_get_tests_passed()	Message Digest	Power-On

Table 22: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Software Integrity Test	KAT	SW/FW Integrity	On Demand	Manually

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC-Encrypt (4588)	KAT	CAST	On Demand	Manually
AES-CBC-Decrypt (4588)	KAT	CAST	On Demand	Manually
AES-CTR Encrypt (4588)	KAT	CAST	On Demand	Manually
AES-CTR Decrypt (4588)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB Encrypt (4588)	KAT	CAST	On Demand	Manually
AES-ECB Decrypt (4588)	KAT	CAST	On Demand	Manually
AES-CBC Encrypt (4589)	KAT	CAST	On Demand	Manually
AES-CBC Decrypt (4589)	KAT	CAST	On Demand	Manually
AES-CBC-CS3 Encrypt	KAT	CAST	On Demand	Manually
AES-CBC-CS3 Decrypt	KAT	CAST	On Demand	Manually
AES-CCM Encrypt	KAT	CAST	On Demand	Manually
AES-CCM Decrypt	KAT	CAST	On Demand	Manually
AES-CMAC (A4589)	KAT	CAST	On Demand	Manually
AES-CTR Encrypt (4589)	KAT	CAST	On Demand	Manually
AES-CTR Decrypt (4589)	KAT	CAST	On Demand	Manually
AES-ECB Encrypt (4589)	KAT	CAST	On Demand	Manually
AES-ECB Decrypt (4589)	KAT	CAST	On Demand	Manually
AES-GCM Encrypt	KAT	CAST	On Demand	Manually
AES-GCM Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Decryt	KAT	CAST	On Demand	Manually
Counter DRBG (A4589)	KAT	CAST	On Demand	Manually
Hash DRBG (A4589)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4589)	KAT	CAST	On Demand	Manually
Entropy	RCT, APT	CAST	On Demand	Manually
HMAC-SHA-1 (A4588)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-224 (A4588)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4588)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A4589)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A4589)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4589)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A4589)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4589)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A4589)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A4589)	KAT	CAST	On Demand	Manually
HMAC-SHA3-384 (A4589)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A4589)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A4589)	KAT	CAST	On Demand	Manually
SHA-1 (A4588)	KAT	CAST	On Demand	Manually
SHA2-224 (A4588)	KAT	CAST	On Demand	Manually
SHA2-256 (A4588)	KAT	CAST	On Demand	Manually
SHA-1 (A4589)	KAT	CAST	On Demand	Manually
SHA2-224 (A4589)	KAT	CAST	On Demand	Manually
SHA2-256 (A4589)	KAT	CAST	On Demand	Manually
SHA2-384 (A4589)	KAT	CAST	On Demand	Manually
SHA2-512 (A4589)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA3-224 (A4589)	KAT	CAST	On Demand	Manually
SHA3-256 (A4589)	KAT	CAST	On Demand	Manually
SHA3-384 (A4589)	KAT	CAST	On Demand	Manually
SHA3-512 (A4589)	KAT	CAST	On Demand	Manually

Table 24: Conditional Periodic Information

The operator may invoke periodic self-tests by power cycling the module. It is recommended that periodic self-testing be performed weekly.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
ES1	The module fails pre-operational self-tests, conditional self- tests, or authentication.	The Module enters the FIPS_error state	Power cycle the module	fips140_get_error()

Table 25: Error States

10.5 Operator Initiation of Self-Tests

Self-tests may be initiated on demand by power cycling the module.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

No end user action is required to startup the module in an approved mode for operation. The module is built into the Wave Relay® OS and delivered in Persistent Systems' Wave Relay® Solutions. There is no standalone delivery of the module as a software hybrid module.

Persistent Systems' internal development process guarantees that the correct version of the module is installed within its intended device OS version.

Installation and Initialization:

The module is pre-installed within the Persistent Systems Solutions, which include the MPU5, Embedded Module, Embedded Module lite, GVR5, or Integrated Antenna Series. No further initialization of the module is required. Upon powering on the hardware platform, the module will automatically perform pre-operational and conditional self-tests in accordance with FIPS 140-3 requirements.

Delivery:
The module is pre-installed within the Persistent Systems product offerings. The Persistent Systems products are distributed using a trusted courier and packaging must be inspected upon delivery.

11.2 Administrator Guidance

There are no specific management activities required of the Crypto Officer Role to ensure that the module runs securely. However, if any irregular activity is noticed or the module is consistently reporting errors, then Persistent Systems Support should be contacted.

11.3 Non-Administrator Guidance

There are no specific management activities required of the Crypto Officer Role to ensure that the module runs securely. However, if any irregular activity is noticed or the module is consistently reporting errors, then Persistent Systems Support should be contacted.

11.4 Design and Rules

Rules of Operation

1. The Module provides one distinct operator roles: Cryptographic Officer.
2. The Module clears previous authentications on power cycle.
3. An operator does not have access to any cryptographic services prior to assuming an authorized role.
4. The Module allows the operator to initiate power-up self-tests by power cycling the Module.
5. All self-tests do not require any operator action.
6. Data output is inhibited during self-tests, zeroisation, 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 SSPs are zeroised by the zeroisation service.
9. The Module does not support concurrent operators.
10. The Module does not support a maintenance interface or role.
11. The Module does not support manual SSP establishment method.
12. The Module does not have any proprietary external input/output devices used for entry/output of data.
13. The Module does not store any plaintext CSPs
14. The Module does not output intermediate key values.
15. The Module does not provide bypass services or ports/interfaces.

11.6 End of Life

The module must be zeroised and returned to the manufacturer.

12 Mitigation of Other Attacks

The Module does not implement any mitigation method against other attacks.

References and Definitions

The following standards are referred to in this Security Policy.

Table 26 – References

Abbreviation	Full Specification Name
[FIPS140-3]	*Security Requirements for Cryptographic Modules*, March 22, 2019
[ISO19790]	*International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017*
[ISO24759]	*International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015*
[IG]	*Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, <date>*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Revision 2, March 2019*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[202]	*FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202, August 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38B]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005*
[38C]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Special Publication 800-38C, May 2004*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[38E]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, Special Publication 800-38E, January 2010*

Abbreviation	Full Specification Name
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, Revision 1, June 2015.*
[90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.*

Table 27 – Acronyms and Definitions

Acronym	Definition
APT	Adaptative Proportion Test
KAT	Know Answer Test
RCT	Repetition Count Test
SSP	Sensitive Security Parameter