Persistent Systems, LLC

Wave Relay® User Space Crypto Module

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.2
Date: September 29, 2025

Table of Contents

1 – General 4
1.1 Overview 4
1.2 Security Levels 4
2 – Cryptographic Module Specification 5
2.1 Description 5
2.2 Tested and Vendor Affirmed Module Version and Identification 6
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 9
2.6 Security Function Implementations 16
2.7 Algorithm Specific Information 41
2.8 RBG and Entropy 41
2.9 Key Generation 42
2.10 Key Establishment 42
2.11 Industry Protocols 42
3 Cryptographic Module Interfaces 43
3.1 Ports and Interfaces 43
4 Roles, Services, and Authentication 43
4.1 Authentication Methods 44
4.2 Roles 44
4.3 Approved Services 44
4.4 Non-Approved Services 49
4.5 External Software/Firmware Loaded 49
5 Software/Firmware Security 49
5.1 Integrity Techniques 49
5.2 Initiate on Demand 50
6 Operational Environment 50
6.1 Operational Environment Type and Requirements 50
6.2 Configuration Settings and Restrictions 50
7 Physical Security 52
8 Non-Invasive Security 52
9 Sensitive Security Parameters Management 52
9.1 Storage Areas 52
9.2 SSP Input-Output Methods 52
9.3 SSP Zeroization Methods 53

9.4 SSPs 54
10 Self-Tests 61
10.1 Pre-Operational Self-Tests 61
10.2 Conditional Self-Tests 61
10.3 Periodic Self-Test Information 65
10.4 Error States 67
10.5 Operator Initiation of Self-Tests 67
11 Life-Cycle Assurance 67
11.1 Installation, Initialization, and Startup Procedures 67
11.2 Administrator Guidance 67
11.3 Non-Administrator Guidance 68
11.4 Design and Rules 68
Rules of Operation 68
11.6 End of Life 68
12 Mitigation of Other Attacks 68
References and Definitions 70

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) 7
Table 3: Tested Operational Environments - Software, Firmware, Hybrid 8
Table 4: Modes List and Description 9
Table 5: Approved Algorithms 14
Table 6: Vendor-Affirmed Algorithms 15
Table 7: Non-Approved, Not Allowed Algorithms 15
Table 8: Security Function Implementations 40
Table 9: Ports and Interfaces 43
Table 10: Authentication Methods 44
Table 11: Roles 44
Table 12: Approved Services 49
Table 13: Non-Approved Services 49
Table 14: Storage Areas 52
Table 15: SSP Input-Output Methods 53
Table 16: SSP Zeroization Methods 53
Table 17: SSP Table 1 56
Table 18: SSP Table 2 59
Table 19: Pre-Operational Self-Tests 61
Table 20: Conditional Self-Tests 65
Table 21: Pre-Operational Periodic Information 65
Table 22: Conditional Periodic Information 66
Table 23: Error States 67
Table 24 – References 70
Table 25 – Acronyms and Definitions 70

List of Figures

Figure 1 Logical Cryptographic Boundary and Physical Perimeter 6

1 – General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version 1.0 of the Persistent Systems LLC Wave Relay® User 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:

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	N/A
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® User Space Crypto Module, hereafter denoted as the "module", is a Software cryptographic module embedded in the Wave Relay® System that provides FIPS validated cryptographic algorithms which are used by user space system services & protocols (e.g., TLS, 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 heat of the moment.

Module Type: Software

Module Embodiment: SingleChip

Module Characteristics:

Cryptographic Boundary:

The TOEPP of the module is depicted in Figure 1. The Module is a single-chip embodiment. The cryptographic boundary is outlined in red and is defined as a dynamic software library (fips.so).

The following block diagram details the module's boundaries:

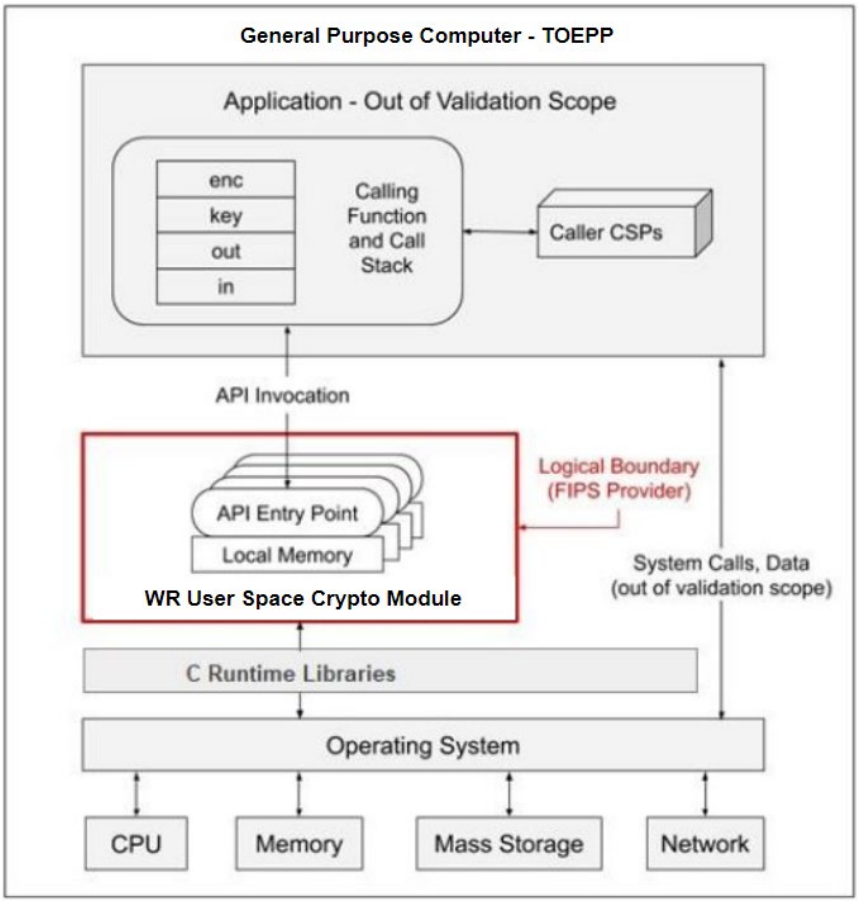

Figure 1 Logical Cryptographic Boundary and Physical Perimeter

2.2 Tested and Vendor Affirmed Module Version and Identification

N/A for this module.

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 User Space Crypto Module	1.0		HMAC-SHA2-256

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

Tested Operational Environments - Software, Firmware, Hybrid:

Wave Relay® User 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, MCIMX6Q6AVT10AD	Yes		1.0
Wave Relay® OS 2.2	Embedded Module	MCIMX6Q7CZK08AE, MSCMMX6QZCK08AB	Yes		1.0
Wave Relay® OS 2.2	Embedded Module lite	MCIMX6Q7CZK08AE, MSCMMX6QZCK08AB	Yes		1.0
Wave Relay® OS 2.2	GVR5	MCIMX6Q7CZK08AE	Yes		1.0
Wave Relay® OS 2.2	Integrated Antenna Series	MCIMX6Q7CZK08AE	Yes		1.0

Table 3: Tested Operational Environments - Software, Firmware, Hybrid

N/A for this module.

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. The Module's status output will include a "FIPS Indicator" line. If this line explicitly states "not-approved", then the Module is in the Non-Approved state; otherwise, the line will be blank, indicating the Approved state.

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	FIPS Indicator:
Non-Approved	The module is capable of non-approved services in the non-approved mode of operation only.	Non-Approved	FIPS Indicator: not-approved

Table 4: 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® User Space Crypto Module version 1.0 (Cert. #A5177)

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

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5177	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS1	A5177	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS2	A5177	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS3	A5177	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A5177	Key Length - 128, 192, 256	SP 800-38C
AES-CFB1	A5177	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A5177	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A5177	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-CMAC	A5177	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A5177	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5177	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A5177	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	A5177	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-KW	A5177	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KWP	A5177	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A5177	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A5177	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
Counter DRBG	A5177	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - No, Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A5177	Curve - B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A5177	Curve - B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571, P-192, P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A5177	Component - No, Yes Curve - B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A5177	Component - No, Yes Curve - B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571, P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
Hash DRBG	A5177	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A5177	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC-SHA-1	A5177	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A5177	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5177	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A5177	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A5177	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/224	A5177	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A5177	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA3-224	A5177	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA3-256	A5177	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA3-384	A5177	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA3-512	A5177	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
KAS-ECC CDH-Component SP800-56Ar3 (CVL)	A5177	Curve - B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A5177	Domain Parameter Generation Methods - B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A5177	Domain Parameter Generation Methods - FB, FC, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
KAS-IFC-SSC	A5177	Modulo - 2048, 3072, 4096, 6144, 8192 Key Generation Methods - rsakpg1-basic, rsakpg1-crt, rsakpg1-prime-factor, rsakpg2-basic, rsakpg2-crt, rsakpg2-prime-factor Scheme - KAS1 - KAS Role - initiator, responder KAS2 - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDA HKDF SP800-56Cr2	A5177	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-8192 Increment 8 HMAC Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512	SP 800-56C Rev. 2
KDA OneStep SP800-56Cr2	A5177	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-8192 Increment 8	SP 800-56C Rev. 2
KDA TwoStep SP800-56Cr2	A5177	MAC Salting Methods - default, random KDF Mode - feedback Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-8192 Increment 8	SP 800-56C Rev. 2
KDF ANS 9.42 (CVL)	A5177	KDF Type - DER Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512 Key Data Length - Key Data Length: 8-4096 Increment 8	SP 800-135 Rev. 1
KDF ANS 9.63 (CVL)	A5177	Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 Key Data Length - Key Data Length: 128, 4096	SP 800-135 Rev. 1
KDF IKEv2 (CVL)	A5177	Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 224, 8192 Derived Keying Material Length - Derived Keying Material Length: 160, 16384 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF SP800-108	A5177	KDF Mode - Counter, Feedback Supported Lengths - Supported Lengths: 8-4096 Increment 8	SP 800-108 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
KDF SSH (CVL)	A5177	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KMAC-128	A5177	Message Length - Message Length: 0-65536 Increment 8 Key Data Length - Key Data Length: 128-1024 Increment 8	SP 800-185
KMAC-256	A5177	Message Length - Message Length: 0-65536 Increment 8 Key Data Length - Key Data Length: 128-1024 Increment 8	SP 800-185
KTS-IFC	A5177	Modulo - 2048, 3072, 4096, 6144, 8192 Key Generation Methods - rsakpg1-basic, rsakpg1-crt, rsakpg1-prime-factor, rsakpg2-basic, rsakpg2-crt, rsakpg2-prime-factor Scheme - KTS-OAEP-basic - KAS Role - initiator, responder Key Transport Method - Key Length - 1024	SP 800-56B Rev. 2
PBKDF	A5177	Iteration Count - Iteration Count: 1-10000 Increment 1 Password Length - Password Length: 8-128 Increment 8	SP 800-132
RSA KeyGen (FIPS186-4)	A5177	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A5177	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA Signature Primitive (CVL)	A5177	Private Key Format - crt	FIPS 186-4
RSA SigVer (FIPS186-4)	A5177	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
Safe Primes Key Generation	A5177	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3
Safe Primes Key Verification	A5177	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3
SHA-1	A5177	Message Length - Message Length: 160, 0-65536 Increment 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-224	A5177	Message Length - Message Length: 224, 0-65536 Increment 8	FIPS 180-4
SHA2-256	A5177	Message Length - Message Length: 256, 0-65536 Increment 8	FIPS 180-4
SHA2-384	A5177	Message Length - Message Length: 384, 0-65536 Increment 8	FIPS 180-4
SHA2-512	A5177	Message Length - Message Length: 512, 0-65536 Increment 8	FIPS 180-4
SHA2-512/224	A5177	Message Length - Message Length: 224, 0-65536 Increment 8	FIPS 180-4
SHA2-512/256	A5177	Message Length - Message Length: 256, 0-65536 Increment 8	FIPS 180-4
SHA3-224	A5177	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-256	A5177	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-384	A5177	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-512	A5177	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHAKE-128	A5177	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SHAKE-256	A5177	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
TLS v1.2 KDF RFC7627 (CVL)	A5177	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
TLS v1.3 KDF (CVL)	A5177	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE, PSK, PSK-DHE	SP 800-135 Rev. 1

Table 5: Approved Algorithms

ApprovedAlgorithmsTable From Web Cryptik ApprovedAlgorithmsTable

Vendor-Affirmed Algorithms:

The Module supports SP800-133rev2, CKG, as the sole vendor affirmed cryptographic algorithm.

- Cryptographic key generation – In compliance with Sections 4 NIST SP 800-133rev2, the module uses its Approved DRBG to generate symmetric keys and the seed used for asymmetric keys without any post-processing.

Name	Properties	Implementation	Reference
CKG - Symmetric and Asymmetric	Key Type:Symmetric and Asymmetric	N/A	SP800-133rev2, Section 4, Example 1

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

The module does not support 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

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
BCU	BC-UnAuth	Symmetric Data Encryption/Decryption	Publication:FIPS 197	AES-CBC: (A5177) Key Length: 128, 192, 256 AES-CBC-CS1: (A5177) Key Length: 128, 192, 256 AES-CBC-CS2: (A5177) Key Length: 128, 192, 256 AES-CBC-CS3: (A5177) Key Length: 128, 192, 256 AES-CFB128: (A5177) Key Length: 128, 192, 256 AES-CFB8: (A5177) Key Length: 128, 192, 256 AES-CTR: (A5177) Key Length: 128, 192, 256 AES-ECB: (A5177) Key Length: 128, 192, 256 AES-XTS Testing Revision 2.0: (A5177) Key Length: 128, 256 AES-OFB: (A5177) Key Length: 128, 192, 256 AES-CFB1: (A5177) Key Length: 128, 192, 256
BCA	BC-Auth	Authenticated Symmetric Encryption/Decryption	Publications:FIPS197, SP800-38C, SP800-38D, SP800-38F	AES-CCM: (A5177) Key Length: 128, 192, 256 AES-GCM: (A5177) Key Length: 128, 192, 256

Name	Type	Description	Properties	Algorithms
				AES-KW: (A5177) Key Length: 128, 192, 256 AES-KWP: (A5177) Key Length: 128, 192, 256
SigVer	DigSig-SigVer	Signature Verification	Publication:186-4	ECDSA SigVer (FIPS186-4): (A5177) Capabilities: Capabilities: Curve: P-192 Hash Algorithm: SHA-1 Capabilities: Curve: P-224 Hash Algorithm: SHA-1 Capabilities: Curve: P-256 Hash Algorithm: SHA-1 Capabilities: Curve: P-384 Hash Algorithm: SHA-1 Capabilities: Curve: P-521 Hash Algorithm: SHA-1 Capabilities: Curve: K-163 Hash Algorithm: SHA-1 Capabilities: Curve: K-233 Hash Algorithm: SHA-1 Capabilities: Curve: K-283 Hash Algorithm: SHA-1 Capabilities: Curve: K-409 Hash Algorithm: SHA-1 Capabilities: Curve: K-571 Hash Algorithm: SHA-1 Capabilities: Curve: B-163 Hash Algorithm: SHA-1 Capabilities: Curve: B-233 Hash Algorithm: SHA-1 Capabilities: Curve: B-283 Hash Algorithm: SHA-1 Capabilities: Curve: B-409 Hash Algorithm: SHA-1 Capabilities: Curve: B-571 Hash Algorithm: SHA-1 Capabilities: Curve: P-192

Name	Type	Description	Properties	Algorithms
				Hash Algorithm: SHA2-224 Capabilities: Curve: P-224 Hash Algorithm: SHA2-224 Capabilities: Curve: P-256 Hash Algorithm: SHA2-224 Capabilities: Curve: P-384 Hash Algorithm: SHA2-224 Capabilities: Curve: P-521 Hash Algorithm: SHA2-224 Capabilities: Curve: K-163 Hash Algorithm: SHA2-224 Capabilities: Curve: K-233 Hash Algorithm: SHA2-224 Capabilities: Curve: K-283 Hash Algorithm: SHA2-224 Capabilities: Curve: K-409 Hash Algorithm: SHA2-224 Capabilities: Curve: K-571 Hash Algorithm: SHA2-224 Capabilities: Curve: B-163 Hash Algorithm: SHA2-224 Capabilities: Curve: B-233 Hash Algorithm: SHA2-224 Capabilities: Curve: B-283 Hash Algorithm: SHA2-224 Capabilities: Curve: B-409 Hash Algorithm: SHA2-224 Capabilities: Curve: B-571 Hash Algorithm: SHA2-224 Capabilities: Curve: P-192 Hash Algorithm: SHA2-256 Capabilities: Curve: P-224 Hash Algorithm: SHA2-256 Capabilities: Curve: P-256 Hash Algorithm: SHA2-256 Capabilities: Curve: P-384 Hash Algorithm: SHA2-256 Capabilities: Curve: P-521 Hash

Name	Type	Description	Properties	Algorithms
				Algorithm: SHA2-256 Capabilities: Curve: K-163 Hash Algorithm: SHA2-256 Capabilities: Curve: K-233 Hash Algorithm: SHA2-256 Capabilities: Curve: K-283 Hash Algorithm: SHA2-256 Capabilities: Curve: K-409 Hash Algorithm: SHA2-256 Capabilities: Curve: K-571 Hash Algorithm: SHA2-256 Capabilities: Curve: B-163 Hash Algorithm: SHA2-256 Capabilities: Curve: B-233 Hash Algorithm: SHA2-256 Capabilities: Curve: B-283 Hash Algorithm: SHA2-256 Capabilities: Curve: B-409 Hash Algorithm: SHA2-256 Capabilities: Curve: B-571 Hash Algorithm: SHA2-256 Capabilities: Curve: P-192 Hash Algorithm: SHA2-384 Capabilities: Curve: P-224 Hash Algorithm: SHA2-384 Capabilities: Curve: P-256 Hash Algorithm: SHA2-384 Capabilities: Curve: P-384 Hash Algorithm: SHA2-384 Capabilities: Curve: P-521 Hash Algorithm: SHA2-384 Capabilities: Curve: K-163 Hash Algorithm: SHA2-384 Capabilities: Curve: K-233 Hash Algorithm: SHA2-384 Capabilities: Curve: K-283 Hash Algorithm: SHA2-384 Capabilities: Curve: K-409 Hash Algorithm:

Name	Type	Description	Properties	Algorithms
				SHA2-384 Capabilities: Curve: K-571 Hash Algorithm: SHA2-384 Capabilities: Curve: B-163 Hash Algorithm: SHA2-384 Capabilities: Curve: B-233 Hash Algorithm: SHA2-384 Capabilities: Curve: B-283 Hash Algorithm: SHA2-384 Capabilities: Curve: B-409 Hash Algorithm: SHA2-384 Capabilities: Curve: B-571 Hash Algorithm: SHA2-384 Capabilities: Curve: P-192 Hash Algorithm: SHA2-512 Capabilities: Curve: P-224 Hash Algorithm: SHA2-512 Capabilities: Curve: P-256 Hash Algorithm: SHA2-512 Capabilities: Curve: P-384 Hash Algorithm: SHA2-512 Capabilities: Curve: P-521 Hash Algorithm: SHA2-512 Capabilities: Curve: K-163 Hash Algorithm: SHA2-512 Capabilities: Curve: K-233 Hash Algorithm: SHA2-512 Capabilities: Curve: K-283 Hash Algorithm: SHA2-512 Capabilities: Curve: K-409 Hash Algorithm: SHA2-512 Capabilities: Curve: K-571 Hash Algorithm: SHA2-512 Capabilities: Curve: B-163 Hash Algorithm: SHA2-512 Capabilities: Curve: B-233 Hash Algorithm: SHA2-512 Capabilities: Curve: B-283 Hash Algorithm: SHA2-512

Name	Type	Description	Properties	Algorithms
				Capabilities: Curve: B-409 Hash Algorithm: SHA2-512 Capabilities: Curve: B-571 Hash Algorithm: SHA2-512 Capabilities: Curve: P-192 Hash Algorithm: SHA2-512/224 Capabilities: Curve: P-224 Hash Algorithm: SHA2-512/224 Capabilities: Curve: P-256 Hash Algorithm: SHA2-512/224 Capabilities: Curve: P-384 Hash Algorithm: SHA2-512/224 Capabilities: Curve: P-521 Hash Algorithm: SHA2-512/224 Capabilities: Curve: K-163 Hash Algorithm: SHA2-512/224 Capabilities: Curve: K-233 Hash Algorithm: SHA2-512/224 Capabilities: Curve: K-283 Hash Algorithm: SHA2-512/224 Capabilities: Curve: K-409 Hash Algorithm: SHA2-512/224 Capabilities: Curve: K-571 Hash Algorithm: SHA2-512/224 Capabilities: Curve: B-163 Hash Algorithm: SHA2-512/224 Capabilities: Curve: B-233 Hash Algorithm: SHA2-512/224 Capabilities: Curve: B-283 Hash Algorithm: SHA2-512/224 Capabilities: Curve: B-409 Hash Algorithm: SHA2-512/224 Capabilities: Curve: B-571 Hash

Name	Type	Description	Properties	Algorithms
				Algorithm: SHA2-512/224 Capabilities: Curve: P-192 Hash Algorithm: SHA2-512/256 Capabilities: Curve: P-224 Hash Algorithm: SHA2-512/256 Capabilities: Curve: P-256 Hash Algorithm: SHA2-512/256 Capabilities: Curve: P-384 Hash Algorithm: SHA2-512/256 Capabilities: Curve: P-521 Hash Algorithm: SHA2-512/256 Capabilities: Curve: K-163 Hash Algorithm: SHA2-512/256 Capabilities: Curve: K-233 Hash Algorithm: SHA2-512/256 Capabilities: Curve: K-283 Hash Algorithm: SHA2-512/256 Capabilities: Curve: K-409 Hash Algorithm: SHA2-512/256 Capabilities: Curve: K-571 Hash Algorithm: SHA2-512/256 Capabilities: Curve: B-163 Hash Algorithm: SHA2-512/256 Capabilities: Curve: B-233 Hash Algorithm: SHA2-512/256 Capabilities: Curve: B-283 Hash Algorithm: SHA2-512/256 Capabilities: Curve: B-409 Hash Algorithm: SHA2-512/256 Capabilities: Curve: B-571 Hash Algorithm: SHA2-512/256 RSA SigVer (FIPS186-4): (A5177)

Name	Type	Description	Properties	Algorithms
				Capabilities: Signature Type: PKCS 1.5 Properties: Modulo: 1024 Hash Pair: Hash Algorithm: SHA-1 Hash Pair: Hash Algorithm: SHA2-224 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Hash Pair: Hash Algorithm: SHA2-512/224 Hash Pair: Hash Algorithm: SHA2-512/256 Properties: Modulo: 2048 Hash Pair: Hash Algorithm: SHA-1 Hash Pair: Hash Algorithm: SHA2-224 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Hash Pair: Hash Algorithm: SHA2-512/224 Hash Pair: Hash Algorithm: SHA2-512/256 Properties: Modulo: 3072 Hash Pair: Hash Algorithm: SHA-1 Hash Pair: Hash Algorithm: SHA2-224 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Hash Pair: Hash Algorithm: SHA2-512/224 Hash Pair: Hash Algorithm: SHA2-512/256 Properties: Modulo: 4096 Hash Pair: Hash Algorithm: SHA-1 Hash Pair: Hash Algorithm: SHA2-224 Hash Pair: Hash

Name	Type	Description	Properties	Algorithms
				Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Hash Pair: Hash Algorithm: SHA2-512/224 Hash Pair: Hash Algorithm: SHA2-512/256 Capabilities: Signature Type: PKCSPSS Properties: Modulo: 1024 Hash Pair: Hash Algorithm: SHA-1 Salt Length: 20 Hash Pair: Hash Algorithm: SHA2-224 Salt Length: 24 Hash Pair: Hash Algorithm: SHA2-256 Salt Length: 32 Hash Pair: Hash Algorithm: SHA2-384 Salt Length: 48 Hash Pair: Hash Algorithm: SHA2-512 Salt Length: 62 Hash Pair: Hash Algorithm: SHA2-512/224 Salt Length: 24 Hash Pair: Hash Algorithm: SHA2-512/256 Salt Length: 32 Properties: Modulo: 2048 Hash Pair: Hash Algorithm: SHA-1 Salt Length: 20 Hash Pair: Hash Algorithm: SHA2-224 Salt Length: 24 Hash Pair: Hash Algorithm: SHA2-256 Salt Length: 32 Hash Pair: Hash Algorithm: SHA2-384 Salt Length: 48 Hash Pair: Hash Algorithm: SHA2-512 Salt Length: 64 Hash Pair: Hash Algorithm: SHA2-512/224 Salt Length: 24 Hash Pair: Hash Algorithm: SHA2-512/256 Salt

Name	Type	Description	Properties	Algorithms
				Length: 32 Properties: Modulo: 3072 Hash Pair: Hash Algorithm: SHA-1 Salt Length: 20 Hash Pair: Hash Algorithm: SHA2-224 Salt Length: 24 Hash Pair: Hash Algorithm: SHA2-256 Salt Length: 32 Hash Pair: Hash Algorithm: SHA2-384 Salt Length: 48 Hash Pair: Hash Algorithm: SHA2-512 Salt Length: 64 Hash Pair: Hash Algorithm: SHA2-512/224 Salt Length: 24 Hash Pair: Hash Algorithm: SHA2-512/256 Salt Length: 32 Properties: Modulo: 4096 Hash Pair: Hash Algorithm: SHA-1 Salt Length: 20 Hash Pair: Hash Algorithm: SHA2-224 Salt Length: 24 Hash Pair: Hash Algorithm: SHA2-256 Salt Length: 32 Hash Pair: Hash Algorithm: SHA2-384 Salt Length: 48 Hash Pair: Hash Algorithm: SHA2-512 Salt Length: 64 Hash Pair: Hash Algorithm: SHA2-512/224 Salt Length: 24 Hash Pair: Hash Algorithm: SHA2-512/256 Salt Length: 32 Public Exponent Mode: Random
AKP-KG	AsymKeyPair-KeyGen	Asymmetric Key Pair Generation	Publication:SP800-56Br2, FIPS 186-4	ECDSA KeyGen (FIPS186-4): (A5177) Curves:: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571,

Name	Type	Description	Properties	Algorithms
				P-224, P-256, P-384, P-521 RSA KeyGen (FIPS186-4): (A5177) Modulo: 2048, 3072, 4096 KTS-IFC: (A5177) Modulo: 2048, 3072, 4096, 6144, 8192 CKG - Symmetric and Asymmetric: () Safe Primes Key Generation: (A5177)
AKP-DP	AsymKeyPair-DomPar	Domain Parameter Generation	Publications:SP800-56Ar3	KAS-ECC-SSC Sp800-56Ar3: (A5177) Methods: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521 KAS-FFC-SSC Sp800-56Ar3: (A5177) Methods: FB, FC, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192
AKP-KV	AsymKeyPair-KeyVer	ECDSA Key Verification	Publication:FIPS186-4	ECDSA KeyVer (FIPS186-4): (A5177) Curve: B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571, P-192, P-224, P-256, P-384, P-521 Safe Primes Key Verification: (A5177)

Name	Type	Description	Properties	Algorithms
AKV-PKV	AsymKeyPair-PubKeyVal	Public Key Validation	Publication:FIPS 186-4	KTS-IFC: (A5177) Modulo: 2048, 3072, 4096, 6144, 8192
SigGen	DigSig-SigGen	Signature Generation and Signature Primitive	Publication:FIPS 186-4	ECDSA SigGen (FIPS186-4): (A5177) Capabilities: Capabilities: Curve: P-224 Hash Algorithm: SHA2-224 Capabilities: Curve: P-256 Hash Algorithm: SHA2-224 Capabilities: Curve: P-384 Hash Algorithm: SHA2-224 Capabilities: Curve: P-521 Hash Algorithm: SHA2-224 Capabilities: Curve: K-233 Hash Algorithm: SHA2-224 Capabilities: Curve: K-283 Hash Algorithm: SHA2-224 Capabilities: Curve: K-409 Hash Algorithm: SHA2-224 Capabilities: Curve: K-571 Hash Algorithm: SHA2-224 Capabilities: Curve: B-233 Hash Algorithm: SHA2-224 Capabilities: Curve: B-283 Hash Algorithm: SHA2-224 Capabilities: Curve: B-409 Hash Algorithm: SHA2-224 Capabilities: Curve: B-571 Hash Algorithm: SHA2-224 Capabilities: Curve: P-224 Hash Algorithm: SHA2-256 Capabilities: Curve: P-256 Hash Algorithm: SHA2-256 Capabilities: Curve: P-384 Hash Algorithm: SHA2-256 Capabilities: Curve: P-521 Hash Algorithm: SHA2-256

Name	Type	Description	Properties	Algorithms
				Capabilities: Curve: K-233 Hash Algorithm: SHA2-256 Capabilities: Curve: K-283 Hash Algorithm: SHA2-256 Capabilities: Curve: K-409 Hash Algorithm: SHA2-256 Capabilities: Curve: K-571 Hash Algorithm: SHA2-256 Capabilities: Curve: B-233 Hash Algorithm: SHA2-256 Capabilities: Curve: B-283 Hash Algorithm: SHA2-256 Capabilities: Curve: B-409 Hash Algorithm: SHA2-256 Capabilities: Curve: B-571 Hash Algorithm: SHA2-256 Capabilities: Curve: P-224 Hash Algorithm: SHA2-384 Capabilities: Curve: P-256 Hash Algorithm: SHA2-384 Capabilities: Curve: P-384 Hash Algorithm: SHA2-384 Capabilities: Curve: P-521 Hash Algorithm: SHA2-384 Capabilities: Curve: K-233 Hash Algorithm: SHA2-384 Capabilities: Curve: K-283 Hash Algorithm: SHA2-384 Capabilities: Curve: K-409 Hash Algorithm: SHA2-384 Capabilities: Curve: K-571 Hash Algorithm: SHA2-384 Capabilities: Curve: B-233 Hash Algorithm: SHA2-384 Capabilities: Curve: B-283 Hash Algorithm: SHA2-384 Capabilities: Curve: B-409 Hash Algorithm: SHA2-384 Capabilities:

Name	Type	Description	Properties	Algorithms
				Curve: B-571 Hash Algorithm: SHA2-384 Capabilities: Curve: P-224 Hash Algorithm: SHA2-512 Capabilities: Curve: P-256 Hash Algorithm: SHA2-512 Capabilities: Curve: P-384 Hash Algorithm: SHA2-512 Capabilities: Curve: P-521 Hash Algorithm: SHA2-512 Capabilities: Curve: K-233 Hash Algorithm: SHA2-512 Capabilities: Curve: K-283 Hash Algorithm: SHA2-512 Capabilities: Curve: K-409 Hash Algorithm: SHA2-512 Capabilities: Curve: K-571 Hash Algorithm: SHA2-512 Capabilities: Curve: B-233 Hash Algorithm: SHA2-512 Capabilities: Curve: B-283 Hash Algorithm: SHA2-512 Capabilities: Curve: B-409 Hash Algorithm: SHA2-512 Capabilities: Curve: B-571 Hash Algorithm: SHA2-512 Capabilities: Curve: P-224 Hash Algorithm: SHA2-512/224 Capabilities: Curve: P-256 Hash Algorithm: SHA2-512/224 Capabilities: Curve: P-384 Hash Algorithm: SHA2-512/224 Capabilities: Curve: P-521 Hash Algorithm: SHA2-512/224 Capabilities: Curve: K-233 Hash Algorithm: SHA2-512/224 Capabilities: Curve: K-283 Hash

Name	Type	Description	Properties	Algorithms
				Algorithm: SHA2-512/224 Capabilities: Curve: K-409 Hash Algorithm: SHA2-512/224 Capabilities: Curve: K-571 Hash Algorithm: SHA2-512/224 Capabilities: Curve: B-233 Hash Algorithm: SHA2-512/224 Capabilities: Curve: B-283 Hash Algorithm: SHA2-512/224 Capabilities: Curve: B-409 Hash Algorithm: SHA2-512/224 Capabilities: Curve: B-571 Hash Algorithm: SHA2-512/224 Capabilities: Curve: P-224 Hash Algorithm: SHA2-512/256 Capabilities: Curve: P-256 Hash Algorithm: SHA2-512/256 Capabilities: Curve: P-384 Hash Algorithm: SHA2-512/256 Capabilities: Curve: P-521 Hash Algorithm: SHA2-512/256 Capabilities: Curve: K-233 Hash Algorithm: SHA2-512/256 Capabilities: Curve: K-283 Hash Algorithm: SHA2-512/256 Capabilities: Curve: K-409 Hash Algorithm: SHA2-512/256 Capabilities: Curve: K-571 Hash Algorithm: SHA2-512/256 Capabilities: Curve: B-233 Hash Algorithm: SHA2-512/256 Capabilities: Curve: B-283 Hash

Name	Type	Description	Properties	Algorithms
				Algorithm: SHA2-512/256 Capabilities: Curve: B-409 Hash Algorithm: SHA2-512/256 Capabilities: Curve: B-571 Hash Algorithm: SHA2-512/256 RSA SigGen (FIPS186-4): (A5177) Capabilities: Signature Type: PKCS 1.5 Properties: Modulo: 2048 Hash Pair: Hash Algorithm: SHA2-224 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Properties: Modulo: 3072 Hash Pair: Hash Algorithm: SHA2-224 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Properties: Modulo: 4096 Hash Pair: Hash Algorithm: SHA2-224 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Capabilities: Signature Type: PKCSPSS Properties: Modulo: 2048 Hash Pair: Hash Algorithm: SHA2-224 Salt Length: 24 Hash Pair: Hash Algorithm: SHA2-256 Salt Length: 32 Hash Pair: Hash Algorithm: SHA2-384 Salt Length: 48 Hash Pair: Hash Algorithm: SHA2-512

Name	Type	Description	Properties	Algorithms
				Salt Length: 64 Hash Pair: Hash Algorithm: SHA2-512/224 Salt Length: 24 Hash Pair: Hash Algorithm: SHA2-512/256 Salt Length: 32 Properties: Modulo: 3072 Hash Pair: Hash Algorithm: SHA2-224 Salt Length: 24 Hash Pair: Hash Algorithm: SHA2-256 Salt Length: 32 Hash Pair: Hash Algorithm: SHA2-384 Salt Length: 48 Hash Pair: Hash Algorithm: SHA2-512 Salt Length: 64 Hash Pair: Hash Algorithm: SHA2-512/224 Salt Length: 24 Hash Pair: Hash Algorithm: SHA2-512/256 Salt Length: 32 Properties: Modulo: 4096 Hash Pair: Hash Algorithm: SHA2-224 Salt Length: 24 Hash Pair: Hash Algorithm: SHA2-256 Salt Length: 32 Hash Pair: Hash Algorithm: SHA2-384 Salt Length: 48 Hash Pair: Hash Algorithm: SHA2-512 Salt Length: 64 RSA Signature Primitive: (A5177) Private Key Format: crt
RAND	DRBG	Random Number Genreation	Publication:SP800-90A	Hash DRBG: (A5177) Mode: SHA-1, SHA2-256, SHA2-512 Counter DRBG: (A5177) Mode: AES-128, AES-192, AES-256 HMAC DRBG: (A5177)

Name	Type	Description	Properties	Algorithms
				Mode: SHA-1, SHA2-256, SHA2-512
Sym-KG	CKG	Cryptographic Key Generation		Counter DRBG: (A5177) Mode: AES-128, AES-192, AES-256 Hash DRBG: (A5177) Mode=: SHA-1, SHA2-256, SHA2-512 HMAC DRBG: (A5177) Mode: SHA-1, SHA2-256, SHA2-512 CKG - Symmetric and Asymmetric: ()
KDF	KAS-135KDF	Application-Specific Key Derivation	Publication:SP800-135	KDF ANS 9.42: (A5177) KDF Type: DER Hash Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512 KDF ANS 9.63: (A5177) Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512 KDF IKEv2: (A5177) Capabilities: Initiator Nonce Length: 128, 2048 Responder Nonce Length: 128, 2048 Diffie-Hellman Shared Secret Length: 224, 8192 Derived Keying Material Length: 160, 16384 Derived Keying Material Child Length: 160, 16384 Hash Algorithm: SHA-1, SHA2-224,

Name	Type	Description	Properties	Algorithms
				SHA2-256, SHA2-384, SHA2-512 KDF SSH: (A5177) Cipher: AES-128, AES-192, AES-256 Hash: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 TLS v1.2 KDF RFC7627: (A5177) Hash Algorithm: SHA2-256, SHA2-384, SHA2-512 TLS v1.3 KDF: (A5177) HMAC Algorithm: SHA2-256, SHA2-384 KDF Running Modes: DHE, PSK, PSK-DHE
KDA	KAS-56CKDF	Key Derivation Methods in Key Establishment Schemes	Publication:SP800-56Cr2	KDA HKDF SP800-56Cr2: (A5177) HMAC Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512 KDA OneStep SP800-56Cr2: (A5177) Auxiliary Function Name: SHA2-512, HMAC-SHA2-224, KMAC-128 KDA TwoStep SP800-56Cr2: (A5177) Capabilities: Fixed Info Pattern: algorithmId||l||uPartyInfo||vPartyInfo Fixed Info Encoding: concatenation KDF Mode: feedback MAC Modes: HMAC-SHA-1, HMAC-SHA2-224,

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, HMAC-SHA2-512/224, HMAC-SHA2-512/256, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512 Fixed Data Order: after fixed data Counter Lengths: 8 The KDF supports an empty IV The KDF requires an empty IV Supported Lengths: 2048
KAS-KG	KAS-KeyGen	KAS Key Generation Methods	Publication:SP800-56Ar3	KAS-ECC-SSC Sp800-56Ar3: (A5177) Domain Parameter Generation Methods: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521 KAS-FFC-SSC Sp800-56Ar3: (A5177) Domain Parameter Generation Methods: FB, FC, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 KAS-IFC-SSC: (A5177) Key Generation Methods: rsakpg1-basic, rsakpg1-crt, rsakpg1-prime-factor, rsakpg2-basic, rsakpg2-crt, rsakpg2-prime-factor
SSC	KAS-SSC	Key Agreement Shared Secret Calculation	IG:IG D.F Scenario 2, path (1)	KAS-FFC-SSC Sp800-56Ar3: (A5177) Domain Parameter Generation

Name	Type	Description	Properties	Algorithms
				Methods: FB, FC, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 KAS-ECC-SSC Sp800-56Ar3: (A5177) Curve: Curve: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521 KAS-IFC-SSC: (A5177) Modulo: 2048, 3072, 4096, 6144, 8192 KAS-ECC CDH-Component SP800-56Ar3: (A5177) Curve: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521
KBKDF	KBKDF	Key Based Key Derivation	Publication:SP800-108	KDF SP800-108: (A5177) Capabilities: KDF Mode: Counter MAC Mode: CMAC-AES128, CMAC-AES192, CMAC-AES256, HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 Supported Lengths: 8-4096 Increment 8 Fixed Data Order: Before Fixed Data Counter Length: 32 Custom Key In Length: 0; KDF Mode: Feedback MAC Mode: CMAC-AES128, CMAC-AES192, CMAC-AES256, HMAC-SHA-1, HMAC-SHA2-224,

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 Supported Lengths: 8-4096 Increment 8 Fixed Data Order: Before Fixed Data Counter Length: 32 Supports Empty IV Requires Empty IV Custom Key In Length: 0
AKP-E	AsymKeyPair-Encap	Asymmetric Key Pair Encapsulation	Standard:SP800-56Br2 IG D.G.:Approved Key Confirmation:No Caveat:Key establishment methodology provides between 112 and 200 bits of security strength	KTS-IFC: (A5177) Modulo: 2048, 3072, 4096, 6144, 8192
AKP-D	AsymKeyPair-Decap	Asymmetric Key Pair Decapsulation	Standard:SP800-56Br2 IG D.G.:Approved Key Confirmation:No Caveat:Key establishment methodology provides between 112 and 200 bits of security strength	KTS-IFC: (A5177) Modulo: 2048, 3072, 4096, 6144, 8192
MAC	MAC	Message Authentication	Publication:FIPS 198, SP800-38B, SP800-38D, SP800-185	AES-CMAC: (A5177) Key Length: 128, 192, 256 AES-GMAC: (A5177) Key Length: 128, 192, 256 HMAC-SHA-1: (A5177)

Name	Type	Description	Properties	Algorithms
				Key Length: 8-524288 Increment 8 HMAC-SHA2-224: (A5177) Key Length: 8-524288 Increment 8 HMAC-SHA2-256: (A5177) Key Length: 8-524288 Increment 8 HMAC-SHA2-384: (A5177) Key Length: 8-524288 Increment 8 HMAC-SHA2-512: (A5177) Key Length: 8-524288 Increment 8 HMAC-SHA2-512/224: (A5177) Key Length: 8-524288 Increment 8 HMAC-SHA2-512/256: (A5177) Key Length: 8-524288 Increment 8 HMAC-SHA3-224: (A5177) Key Length: 8-524288 Increment 8 HMAC-SHA3-256: (A5177) Key Length: 8-524288 Increment 8 HMAC-SHA3-384: (A5177) Key Length: 8-524288 Increment 8 KMAC-256: (A5177) Key Length: 128-1024 Increment 8 KMAC-128: (A5177) Key Length: 128-1024 Increment 8 HMAC-SHA3-512: (A5177) Key Length: 8-524288 Increment 8
PBKDF	PBKDF	Password Based Key Derivation	Publication:SP800-132	PBKDF: (A5177) HMAC Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256
SHS	SHA	Message Digest	Publications:FIPS 180-4, FIPS 202	SHA-1: (A5177) Message Length: 0-65536 Increment 8, 160

Name	Type	Description	Properties	Algorithms
				SHA2-224: (A5177) Message Length: 0-65536 Increment 8, 224 SHA2-256: (A5177) Message Length: 0-65536 Increment 8, 256 SHA2-384: (A5177) Message Length: 0-65536 Increment 8, 384 SHA2-512: (A5177) Message Length: 0-65536 Increment 8, 512 SHA2-512/224: (A5177) Message Length: 0-65536 Increment 8, 224 SHA2-512/256: (A5177) Message Length: 0-65536 Increment 8, 256 SHA3-224: (A5177) Message Length: 0-65536 Increment 8 SHA3-256: (A5177) Message Length: 0-65536 Increment 8 SHA3-384: (A5177) Message Length: 0-65536 Increment 8 SHA3-512: (A5177) Message Length: 0-65536 Increment 8 SHAKE-128: (A5177) Output Length: 16-65536 Increment

Name	Type	Description	Properties	Algorithms
				8 SHAKE-256: (A5177) Output Length: 16-65536 Increment 8

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.

FIPS140-3 IG C.H, Option 2: AES GCM IV Uniqueness

The IV is generated internally at its entirety randomly.

The generation uses an Approved DRBG (Cert. #A5177) 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: XTS-AES Requirements

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

FIPS 140-3 IG D.N: PBKDF Requirements

The module conforms to IG D.N, Option 1a.

The password length is 8 – 128 bytes. The password may be selected from a set of 94 characters. So the total combinations for an 8-character password are 94^8. Thus, the probability of guessing the correct password on a random attempt is 1/94^8.

The iteration count is 1 - 10,000, as determined by the operator.

Keys derived from passwords per SP800-132 may only be used in storage applications.

SHA-1 Usage

Per SP800-131Ar2, the use of SHA-1 is disallowed for digital signature generation, but is permitted for digital signature verification (legacy use) and all non-digital signature applications.

KAS and KTS

The module does not establish SSPs using an approved key agreement scheme (KAS). However, it does offer some or all of the underlying KAS cryptographic functionality to be used by an external operator/application as part of an approved KAS.

The module does not establish SSPs using an approved key transport scheme (KTS). However, it does offer approved authenticated algorithms that can be used by an external operator/application as part of an approved KTS.

2.8 RBG and Entropy

N/A for this module.

The Module uses an entropy source from within the TOEPP, but outside of the cryptographic boundary. The module exercises no control over the source of entropy per IG 9.3.A, Scenario 2B. The size of the entropy provided to the DRBG varies depending on the DRBG mechanism (i.e., HASH, CTR, HMAC) and desired security strength. No assurance of the minimum strength of generated SSPs (e.g., keys).

N/A for this module.

2.9 Key Generation

The module generates both symmetric and asymmetric cryptographic keys using the internal DRBG (CAVP Cert. #A5177).
The module implements key generation methods according to SP 800-133r2 Section 4, Example 1, without the use of V. The key generation methods are specified in the Vendor Affirmed Algorithms table and the Security Function Implementations table. Additionally, the module implements key derivation methods according to Section 6.2 of SP 800-133r2. The key derivation methods are specified in the Security Function Implementations table.

2.10 Key Establishment

The module does not establish SSPs using an approved key agreement scheme (KAS) or key transport scheme (KTS). However, it does offer some or all of the underlying KAS cryptographic functionality and approved authenticated algorithms that can be used by an external operator/application as part of an approved KAS or KTS.
The module supports KAS-ECC-SSC, KAS-FFC-SSC, KAS-IFC-SSC, AES-KW, AES-KWP, and KTS-IFC. **KAS-IFC SSC [56Br2]** - Per [IG] D.F Scenario 1 path (1), compliant the derivation of a shared secret Z in one of the schemes in Sections 8.2 and 8.3 of SP 800-56Brev2.

KAS-SSC [56Ar3] - Per [IG] D.F Scenario 2 path (2), compliant with the derivation of a shared secret Z in one or more of the key agreement schemes in Section 6 of SP 800-56Arev3. Testing is split into (i) testing the computation of the shared secret and (ii) testing the key derivation function used in deriving the keying material comply to IG 2.4.B.

KAS-SSC as a service:
The module does not establish SSPs using an approved key agreement scheme (KAS). However, it does offer some or all of the underlying KAS cryptographic functionality to be used by an external operator/application as part of an approved KAS.

2.11 Industry Protocols

The module does not implement any Industry Protocols. The module is a cryptographic toolkit that may be used in support for Industry Protocols but does not itself implement the protocol.

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, signed, or hashed o Keys to be used in cryptographic services o Random seed material for Module's DRBG o Keying Material to be used as input to key establishment 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, signed, or verified o Hashes o Random Values generated by the module's DRBG o o Keys Established using module's key establishment methods
N/A	Status Output	o API call return values o Status information regarding the module
N/A	Power	N/A

Table 9: 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	SigVer	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 0.3 seconds, which results in a maximum of 200 authentication attempts per minute. The probably of a brute force attack being successful within a given minute is 200/(2^128).

Table 10: 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 11: 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.	OSSL_FIPS_PARAM_INDICATOR	Power	Status	None	Cryptographic Officer - Software Integrity Key: E - CO Authentication Key: E
Show Status	Shows module's status	OSSL_FIPS_PARAM_INDICATOR	None	Status	None	Cryptographic Officer
Show Version	Shows module's versioning information	OSSL_FIPS_PARAM_INDICATOR	None	Module Base Name + Module Version Number	None	Cryptographic Officer
Symmetric Encryption/Decryption	Encryption and decryption of data.	OSSL_FIPS_PARAM_INDICATOR	AES Key, Plaintext or Ciphertext	Plaintext or Ciphertext	BCU BCA	Cryptographic Officer - AES Key: W,E,Z
Keyed MAC	Compute a Message Authentication Code	OSSL_FIPS_PARAM_INDICATOR	Message, HMAC, AES, or KMAC Key	Message Authentication Code	MAC	Cryptographic Officer - AES Key: W,E,Z - MAC Key: W,E,Z
Hash	Compute a Message Digest	OSSL_FIPS_PARAM_INDICATOR	Message	Hash Value	SHS	Cryptographic Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Random Bit Generation	Generate random values	OSSL_FIPS_PARAM_INDICATOR	DRBG Selection	Random Values	RAND	Cryptographic Officer - DRBG-V: W,E,Z - DRBG-C: W,E,Z - DRBG-Key: W,E,Z - DRBG-EI: G,W,E,Z
Signature Generation	Signature Generation	OSSL_FIPS_PARAM_INDICATOR()=1	Private Key, Message	Digital Signature	SigGen	Cryptographic Officer - RSA Private Key: W,E,Z - ECDSA Private Key: W,E,Z
Signature Verification	Signature Verification	OSSL_FIPS_PARAM_INDICATOR	Public Key, Signature	Status	SigVer	Cryptographic Officer - RSA Public Key: W,E,Z - ECDSA Public Key: W,E,Z
Key Generation	Generate asymmetric keys	OSSL_FIPS_PARAM_INDICATOR	Key Attributes,	Private Key,	AKP-KG AKP-	Cryptographic Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	(i.e., RSA, EC)		Key Size	Public Key	DP RAND KAS-KG Sym-KG	- DRBG-V: E,Z - RSA Private Key: G,R,Z - RSA Public Key: G,R,Z - ECDSA Private Key: G,R,Z - ECDSA Public Key: G,R,Z - KAS Private Key: G,R,Z - KAS Public Key: G,R,Z - DRBG-C: E,Z - DRBG-Key: E,Z
Key Verification	Asymmetric Key Verification	OSSL_FIPS_PARAM_INDICATOR	Public Key	Validity	AKP-KV AKV-PKV	Cryptographic Officer - ECDSA Public Key: W,E,Z - KAS Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: W,E,Z
Key Derivation	Derive keys using SP800-56Cr2, SP800-135, SP800-108, or SP800-132 key derivation methods	OSSL_FIPS_PARAM_INDICATOR	Key Material, Passphrase	Key Material	KDF KDA KBKDF PBKDF	Cryptographic Officer - AES Key: W,E,Z - MAC Key: W,E,Z - Key Material: G,R,W,E,Z - Passphrase: W,E,Z
Shared Secret Calculation	Key agreement using KAS-ECC, KAS-FFC, or KAS-IFC	OSSL_FIPS_PARAM_INDICATOR	RSA or KAS Public and Private Keys	Key Material	SSC	Cryptographic Officer - Key Material: G,R,Z - RSA Private Key: W,E,Z - RSA Public Key: W,E,Z - KAS Private Key: W,E,Z - KAS Public Key: W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Key Transport	Key transport using AES-KW or KTS-IFC	OSSL_FIPS_PARAM_INDICATOR	AES Key, RSA Key	Wrapped or Encapsulated Key	BCA AKP-E AKP-D	Cryptographic Officer - AES Key: W,E,Z - RSA Public Key: W,E,Z - RSA Private Key: W,E,Z

Table 12: 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

Table 13: 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 library – binary (fips.so)

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 module is software and as such, physical security requirements do not apply.

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 14: 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	
Input encapsulated (IO3)	Application Software (outside)	System Memory (S1)	Encrypted	Manual	Electronic	AKP-D
Output encapsulated (IO4)	System Memory (S1)	Application Software (outside)	Encrypted	Manual	Electronic	AKP-E
Input wrapped (IO5)	Application Software (outside)	System Memory (S1)	Encrypted	Manual	Electronic	BCA

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Output wrapped (IO6)	System Memory (S1)	Application Software (outside)	Encrypted	Manual	Electronic	BCA

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Z1	Zeroisation upon use	Active overwriting of SSP values with 0s immediately after SSP is no longer needed	Automatic upon use

Table 16: 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	384 - 768 - 128 to 256 bits	ENT - CSP			RAND
DRBG-V	DRBG internal state value (V for all DRBGs)	440 - 888 (Hash_DRBG); 128 (CTR_DRBG); 160-512 (HMAC_DRBG) - 128 to 256	DRBG - CSP	RAND		AKP-KG RAND Sym-KG KAS-KG
DRBG-C	DRBG internal state value (C for HASH_DRBG)	440 - 888 (Hash_DRBG); 128 (CTR_DRBG); 160-512 (HMAC_DRBG) - 128 to 256	DRBG - CSP	RAND		AKP-KG RAND Sym-KG KAS-KG
DRBG-Key	DRBG internal state value (Key for HMAC_DRBG and CTR_DRBG)	128 to 256 bits (CTR_DRBG); 160-512 (HMAC_DRBG) - 128 to 256	DRBG - CSP	RAND		AKP-KG RAND Sym-KG KAS-KG
AES Key	Used for encryption/decryption operations. May also be used for MAC (AES-	128, 192, 256 - 128, 192, 256	Symmetric - CSP			BCU BCA KBKDF MAC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	CMAC, AES-GMAC) or KBKDF.					
MAC Key	Used for Message Authentication (HMAC or KMAC)	HMAC: 8 to 524288 (Increment 8) (Legacy less than 112) KMAC: 128-1024 (increment 8) - 128 to 512	MAC - CSP			KDF KDA KBKDF MAC PBKDF
RSA Private Key	Signature Generation, KTS-IFC, KAS-IFC	2048, 3072, 4096, 6144 (KAS-IFC and KTS-IFC only), 8192 (KAS-IFC and KTS-IFC only) - 112-150	Asymmetric - CSP	AKP-KG		SigGen SSC AKP-D
RSA Public Key	Used for signature verification, KTS-IFC, KAS-IFC	1024 (Legacy), 2048, 3072, 4096, 6144 (KAS-IFC and KTS-IFC only), 8192 (KAS-IFC and KTS-IFC only) - 112-150 (Legacy >112)	Asymmetric - PSP	AKP-KG		SigVer SSC AKP-E
CO Authentication Key	Used for authenticating the CO	3072 - 128	Asymmetric - PSP	At manufacturing		SigVer
Software Integrity Key	Used for Module Integrity	256 - 256	MAC - Neither	At manufacturing		MAC
ECDSA Private Key	Used for signature generation	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521 - 112-256	Asymmetric - CSP	AKP-KG		SigGen
ECDSA Public Key	Used for signature verification	B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571, P-192, P-224, P-256, P-384,	Asymmetric - PSP	AKP-KG		SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		P-521 - 112-256 (Legacy >112)				
KAS Private Key	Used for key agreement (FFC and ECC)	ECC: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521; FFC: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 - 112-256	Asymmetric - CSP	KAS-KG		SSC
KAS Public Key	Used for key agreement (FFC and ECC)	ECC: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521; FFC: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 - 112-256	Asymmetric - PSP	KAS-KG		SSC
Passphrase	Passphrase to be used with PBKDF2	64-1024 - N/A	PBKDF2 - CSP			PBKDF
Key Material	May be intended for or the result of SSC, KDA, KDF, or KTS	Varies - 128 to 256	Key Material - CSP			SSC

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG-EI	Input in plaintext (IO1)	System Memory (S1):Plaintext	Until use completes	Z1	DRBG-V:Used to derive DRBG-C:Used to derive DRBG-Key:Used to derive
DRBG-V		System Memory (S1):Plaintext	Until use completes	Z1	DRBG-EI:Derived From DRBG-C:Used With DRBG-Key:Used With
DRBG-C		System Memory (S1):Plaintext	Until use completes	Z1	DRBG-EI:Derived From DRBG-V:Used With
DRBG-Key		System Memory (S1):Plaintext	Until use completes	Z1	DRBG-EI:Derived From DRBG-V:Used With
AES Key	Input in plaintext (IO1) Output in plaintext (IO2)	System Memory (S1):Plaintext	Until use completes	Z1	
MAC Key	Input in plaintext (IO1) Output in plaintext (IO2)	System Memory (S1):Plaintext	Until use completes	Z1	
RSA Private Key	Input in plaintext (IO1) Output in plaintext (IO2)	System Memory (S1):Plaintext	Until use completes	Z1	RSA Public Key:Paired With
RSA Public Key	Input in plaintext (IO1) Output in plaintext (IO2)	System Memory (S1):Plaintext	Until use completes	Z1	RSA Private Key:Paired With
CO Authentication Key		Binary (S2):Plaintext System Memory (S1):Plaintext	Until use completes	Z1	Software Integrity Key:Protected by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Software Integrity Key		Binary (S2):Plaintext System Memory (S1):Plaintext	Until use completes	Z1	
ECDSA Private Key	Input in plaintext (IO1) Output in plaintext (IO2)	System Memory (S1):Plaintext	Until use completes	Z1	
ECDSA Public Key	Input in plaintext (IO1) Output in plaintext (IO2)	System Memory (S1):Plaintext	Until use completes	Z1	ECDSA Private Key:Paired With
KAS Private Key	Input in plaintext (IO1) Output in plaintext (IO2)	System Memory (S1):Plaintext	Until use completes	Z1	KAS Public Key:Paired With DRBG-State:Generated with Key Material:Establishes
KAS Public Key	Input in plaintext (IO1) Output in plaintext (IO2)	System Memory (S1):Plaintext	Until use completes	Z1	KAS Private Key:Paired With DRBG-State:Generated with Key Material:Establishes
Passphrase	Input in plaintext (IO1)	System Memory (S1):Plaintext	Until use completes	Z1	Key Material:Derives
Key Material	Input in plaintext (IO1) Output in plaintext (IO2) Input encapsulated (IO3) Output encapsulated (IO4) Input wrapped (IO5)	System Memory (S1):Plaintext	Until use completes	Z1	Passphrase:Derived From RSA Private Key:Derived From RSA Public Key:Derived From KAS Private Key:Derived From KAS Public Key:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Output wrapped (IO6)				AES Key:Derived From MAC Key:Derived From

Table 18: 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	verify_integrity_success or verify_integrity failure	HMAC-SHA2-256 Verify

Table 19: 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-GCM Encrypt	Key size: 256 bits	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Encrypt	Power-On

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM Decrypt	Key size: 256 bits	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Decrypt	Power-On
AES-ECB (A5177)	Key size: 128 bits	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Decrypt	Power-On
Counter DRBG (A5177)	Key size: 128	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	instantiation, generate, and reseed	Power-On
Hash DRBG (A5177)	SHA2-256	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	instantiation, generate, and reseed	Power-On
HMAC DRBG (A5177)	SHA1	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	instantiation, generate, and reseed	Power-On
HMAC-SHA2-256 (A5177)	SHA2-256 with 256-bit key	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Generate/Verify	Power-On
KMAC-256 (A5177)	KMAC-256 with 384-bit key	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Generate/Verify	Power-On
RSA SigGen (FIPS186-4) (A5177)	PKCS#1, SHA2-256 with 2048-bit key	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Signature Generation	Power-On
RSA SigVer (FIPS186-4) (A5177)	PKCS#1, SHA2-256 with 2048-bit key	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Signature Verification	Power-On
RSA KeyGen (FIPS186-4) (A5177)	Key Generation	PCT	PCT	OSSL_PROV_PARAM_STATUS = 1 (ok) OSSL_PROV_PARAM_STATUS = 0 (error)	Encrypt/Decrypt	Upon key generation
SHA-1 (A5177)	SHA-1	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Generate/Verify	Power-On
SHA2-512 (A5177)	SHA2-512	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Generate/Verify	Power-On

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA3-256 (A5177)	SHA3-256	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Generate/Verify	Power-On
ECDSA SigGen (FIPS186-4) (A5177)	P-224, B-233 with SHA2-256	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Signature Generation	Power-On
ECDSA SigVer (FIPS186-4) (A5177)	P-224, B-233 with SHA2-256	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Signature Verification	Power-On
KAS-ECC-SSC Sp800-56Ar3 (A5177)	P-256	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Shared Secret Calculation	Power-On
KAS-FFC-SSC Sp800-56Ar3 (A5177)	ffdhe2048	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Shared Secret Calculation	Power-On
Safe Primes Key Generation (A5177)	Key Generation	PCT	PCT	OSSL_PROV_PARAM_STATUS = 1 (ok) OSSL_PROV_PARAM_STATUS = 0 (error)	SP800-56Ar3 PCT	Upon key generation
ECDSA KeyGen (FIPS186-4) (A5177)	Key Generation	PCT	PCT	OSSL_PROV_PARAM_STATUS = 1 (ok) OSSL_PROV_PARAM_STATUS = 0 (error)	Sign/Verify	Upon key generation
TLS v1.2 KDF RFC7627 (A5177)	SHA2-256 with 384-bit secret	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Key Derivation	Power-On

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
TLS v1.3 KDF (A5177)	SHA2-256 with 256-bit Key	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Key Derivation	Power-On
PBKDF (A5177)	HMAC SHA2-256 with 24 character passphrase	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Key Derivation	Power-On
KTS-IFC (A5177)	2048-bit Key	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Encrypt/Decrypt	Power-On
KDF SSH (A5177)	SHA-1 with 1056-bits	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Key Derivation	Power-On
KDF SP800-108 (A5177)	HMAC SHA2-256, Counter Mode, 128-bit. CMAC AES-128, Counter Mode, 128-bit	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Key Derivation	Power-On
KDF IKEv2 (A5177)	SHA-1, 192-bit secret, 160-bit skeyseed	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Key Derivation	Power-On
KDF ANS 9.63 (A5177)	SHA2-256, 192-bit secret	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Key Derivation	Power-On
KDF ANS 9.42 (A5177)	SHA-1, 160-bit secret	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Key Derivation	Power-On
KDA HKDF SP800-56Cr2 (A5177)	HMAC SHA2-256	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Key Derivation	Power-On
KDA OneStep SP800-56Cr2 (A5177)	HMAC SHA2-224 with 448-bit secret	KAT	CAST	SELF_TEST_post success SELF_TEST_post failure	Key Derivation	Power-On

Table 20: 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 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM Encrypt	KAT	CAST	On Demand	Manually
AES-GCM Decrypt	KAT	CAST	On Demand	Manually
AES-ECB (A5177)	KAT	CAST	On Demand	Manually
Counter DRBG (A5177)	KAT	CAST	On Demand	Manually
Hash DRBG (A5177)	KAT	CAST	On Demand	Manually
HMAC DRBG (A5177)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A5177)	KAT	CAST	On Demand	Manually
KMAC-256 (A5177)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A5177)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A5177)	KAT	CAST	On Demand	Manually
RSA KeyGen (FIPS186-4) (A5177)	PCT	PCT	On Demand	Manually
SHA-1 (A5177)	KAT	CAST	On Demand	Manually
SHA2-512 (A5177)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA3-256 (A5177)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A5177)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A5177)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A5177)	KAT	CAST	On Demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A5177)	KAT	CAST	On Demand	Manually
Safe Primes Key Generation (A5177)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A5177)	PCT	PCT	On Demand	Manually
TLS v1.2 KDF RFC7627 (A5177)	KAT	CAST	On Demand	Manually
TLS v1.3 KDF (A5177)	KAT	CAST	On Demand	Manually
PBKDF (A5177)	KAT	CAST	On Demand	Manually
KTS-IFC (A5177)	KAT	CAST	On Demand	Manually
KDF SSH (A5177)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A5177)	KAT	CAST	On Demand	Manually
KDF IKEv2 (A5177)	KAT	CAST	On Demand	Manually
KDF ANS 9.63 (A5177)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A5177)	KAT	CAST	On Demand	Manually
KDA HKDF SP800-56Cr2 (A5177)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A5177)	KAT	CAST	On Demand	Manually

Table 22: 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 error state	Power cycle the module	OSSL_PROV_PARAM_STATUS = 0

Table 23: 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 provides identity-based authentication.
3. The Module clears previous authentications on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The Module allows the operator to initiate power-up self-tests by power cycling the Module.
6. All self-tests do not require any operator action.
7. Data output is inhibited during self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
9. There are no restrictions on which keys or SSPs are zeroized after use.
10. The Module does not support concurrent operators.
11. The Module does not support a maintenance interface or role.
12. The Module does not support manual SSP establishment method.
13. The Module does not have any proprietary external input/output devices used for entry/output of data.
14. The Module does not store any plaintext CSPs.
15. The Module does not output intermediate key values.
16. The Module does not provide bypass services for ports/interfaces.

11.6 End of Life

The module must be zeroized 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 24 – References

Table 25 – Acronyms and Definitions