Microsoft Corporation

Microsoft HSM Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.1

Last Update: 2026-08-10

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

https://www.atsec.com

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
1.3 Additional Information 5
2 Cryptographic Module Specification 6
2.1 Description 6
2.2 Tested and Vendor Affirmed Module Version and Identification 7
2.3 Excluded Components 7
2.4 Modes of Operation 7
2.5 Algorithms 8
2.6 Security Function Implementations 29
2.7 Algorithm Specific Information 35
2.8 RBG and Entropy 37
2.9 Key Generation 37
2.10 Key Establishment 38
2.11 Industry Protocols 38
3 Cryptographic Module Interfaces 39
3.1 Ports and Interfaces 39
4 Roles, Services, and Authentication 40
4.1 Authentication Methods 40
4.2 Roles 42
4.3 Approved Services 42
4.4 Non-Approved Services 54
4.5 External Software/Firmware Loaded 54
5 Software/Firmware Security 55
5.1 Integrity Techniques 55
5.2 Initiate on Demand 55
6 Operational Environment 56
6.1 Operational Environment Type and Requirements 56
7 Physical Security 57
7.1 Mechanisms and Actions Required 57
7.2 EFP/EFT Information 57

7.3 Hardness Testing Temperature Ranges 57
8 Non-Invasive Security 58
9 Sensitive Security Parameters Management 59
9.1 Storage Areas 59
9.2 SSP Input-Output Methods 59
9.3 SSP Zeroization Methods 60
9.4 SSPs 60
9.5 Transitions 67
10 Self-Tests 68
10.1 Pre-Operational Self-Tests 68
10.2 Conditional Self-Tests 68
10.3 Periodic Self-Test Information 73
10.4 Error States 76
11 Life-Cycle Assurance 78
11.1 Installation, Initialization, and Startup Procedures 78
11.2 Administrator Guidance 78
11.3 Non-Administrator Guidance 78
11.4 End of Life 78
12 Mitigation of Other Attacks 79
A Glossary and Abbreviations 80

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Hardware 7
Table 3: Modes List and Description 8
Table 4: Approved Algorithms 28
Table 5: Vendor-Affirmed Algorithms 29
Table 6: Non-Approved, Not Allowed Algorithms 29
Table 7: Security Function Implementations 35
Table 8: Entropy Certificates 37
Table 9: Entropy Sources 37
Table 10: Ports and Interfaces 39
Table 11: Authentication Methods 41
Table 12: Roles 42
Table 13: Approved Services 54
Table 14: Non-Approved Services 54
Table 15: Mechanisms and Actions Required 57
Table 16: EFP/EFT Information 57
Table 17: Hardness Testing Temperatures 57
Table 18: Storage Areas 59
Table 19: SSP Input-Output Methods 60
Table 20: SSP Zeroization Methods 60
Table 21: SSP Table 1 63
Table 22: SSP Table 2 67
Table 23: Conditional Self-Tests 72
Table 24: Conditional Periodic Information 76
Table 25: Error States 77

List of Figures

Figure 1: Module's block diagram 6
Figure 2: Module top level view and physical perimeter 7

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the Microsoft HSM Cryptographic Module. It describes the security rules under which the module must operate and how the module meets the requirements of FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) at overall Security Level 3.

This Non-Proprietary Security Policy may be reproduced and distributed, provided it is kept whole and intact and includes this notice. All other documentation remains proprietary to its respective authors.

1.2 Security Levels

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

Table 1: Security Levels

1.3 Additional Information

The laboratory formatted the vendor-supplied documentation into a consolidated Security Policy document without altering any technical statements. The Security Policy was then refined iteratively throughout conformance testing. The vendor reviewed both intermediate and final versions and approved all content.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use: The Microsoft HSM Cryptographic Module (hereafter referred to as "the module") is a single chip hardware module that provides cryptographic services. It consists of two layers: the HSM layer and the HSP layer, which are accessed through different interfaces as specified in Section 3.1 of this Security Policy.

Module Type: Hardware
Module Embodiment: Single Chip
Module Characteristics:

Cryptographic Boundary: The cryptographic boundary is the entire chip. Figure 1 displays a block diagram of the module.

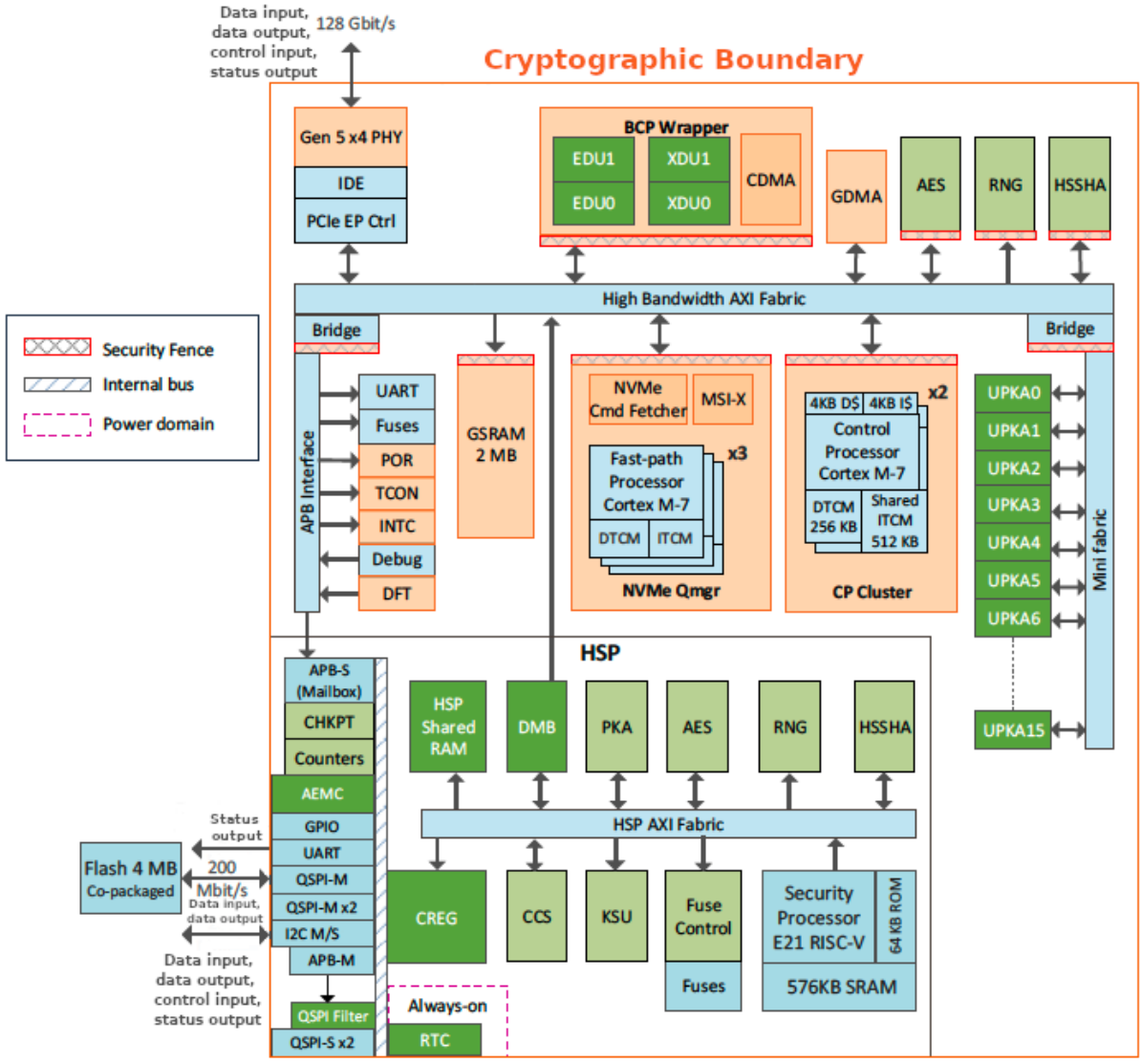

Figure 1: Module's block diagram

Figure 2: Module top level view and physical perimeter

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
M1244265-004 B0	M1244265-004 B0	Version of the ROM FW image executed by the HSP processor: M1244265-004 B0; version of the two RAM FW images executed by the HSP processor: 3.4.2.3-50917001fips (boot-time firmware) and 3.3.6.4-60108004fips (run-time firmware); version of the two RAM FW images executed by the HSM PCI PHY controllers: 3.3.6.4-60108004fips; version of the three RAM FW images executed by the HSM Fast-path processors: 3.3.6.4-60108004fips; version of the RAM FW image executed by the HSM Control processors: 3.3.6.4-60108004fips	1x SiFive E21 RISC-V processor (HSP processor); 2x Microsoft ARM Cortex-M7 processors (called HSM Control processors); 3x Microsoft ARM Cortex-M7 processors (called HSM Fast-path processors); 2x R8051XC2 microcontrollers version 2.24 (called the HSM PCI PHY controller)	N/A

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

The module does not claim any excluded components.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode	Automatically entered whenever an approved service is requested	Approved	Equivalent to the indicator of the requested service
Non-Approved mode	Automatically entered whenever a non-approved service is requested	Non-Approved	Equivalent to the indicator of the requested service

Table 3: Modes List and Description

The module automatically transitions to approved mode after passing all pre-operational and CASTs performed at power-on. No operator intervention is required to reach this point.

Mode Change Instructions and Status:

The module automatically switches between the approved and non-approved modes depending on the services requested by the operator. The status indicator of the mode of operation is equivalent to the indicator of the service that was requested.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A7763	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A4199	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6565	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A7927	Direction - Decrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A7984	Direction - Decrypt, Encrypt IV Generation - External, Internal Key Length - 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 128-4096 Increment 128 AAD Length - AAD Length: 0 IV Generation Mode - 8.2.1	SP 800-38D
AES-KWP	A7927	Direction - Decrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 8-4096 Increment 8	SP 800-38F

Algorithm	CAVP Cert	Properties	Reference
AES-KWP	A7980	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 256 Payload Length - Payload Length: 8-4096 Increment 8	SP 800-38F
AES-XTS Testing Revision 2.0	A7760	Direction - Decrypt, Encrypt Key Length - 256 Payload Length - Payload Length: 128-65536 Increment 128 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
AES-XTS Testing Revision 2.0	A7761	Direction - Decrypt, Encrypt Key Length - 256 Payload Length - Payload Length: 128-65536 Increment 128 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
ECDSA KeyGen (FIPS186-5)	A7764	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A7765	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A7766	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A7767	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A7768	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A7769	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A7770	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A7771	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A7772	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A7773	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A7774	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
ECDSA KeyGen (FIPS186-5)	A7775	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A7776	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A7777	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A7778	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A7779	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A7977	Curve - P-384 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7764	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7765	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7766	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7767	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7768	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7769	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7770	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
		512 Component - Yes	
ECDSA SigGen (FIPS186-5)	A7771	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7772	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7773	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7774	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7775	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7776	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7777	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7778	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7779	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - Yes	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7977	Curve - P-384 Hash Algorithm - SHA2-384 Component - No	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigGen (FIPS186-5)	A7978	Curve - P-384 Hash Algorithm - SHA2-384 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A7976	Component - No Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A7977	Component - No Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A7978	Component - No Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-5
HMAC DRBG	A6566	Prediction Resistance - No Supports Reseed - Yes Mode - SHA2-512 Entropy Input - Entropy Input: 1024 Nonce - Nonce: 0 Personalization String Length - Personalization String Length: 0 Additional Input - Additional Input: 0 Returned Bits - 512	SP 800-90A Rev. 1
HMAC-SHA2-256	A4199	MAC - MAC: 256 Key Length - Key Length: 256	FIPS 198-1
HMAC-SHA2-256	A7928	MAC - MAC: 256 Key Length - Key Length: 256	FIPS 198-1
HMAC-SHA2-256	A7983	MAC - MAC: 256 Key Length - Key Length: 112-4096 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4199	MAC - MAC: 384 Key Length - Key Length: 384	FIPS 198-1
HMAC-SHA2-384	A7928	MAC - MAC: 384 Key Length - Key Length: 384	FIPS 198-1
HMAC-SHA2-384	A7983	MAC - MAC: 384 Key Length - Key Length: 112-4096 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6566	MAC - MAC: 512 Key Length - Key Length: 512	FIPS 198-1
HMAC-SHA2-512	A7928	MAC - MAC: 512 Key Length - Key Length: 512	FIPS 198-1
HMAC-SHA2-512	A7983	MAC - MAC: 512 Key Length - Key Length: 112-4096 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
KAS-ECC-SSC Sp800-56Ar3	A7764	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A7765	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A7766	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A7767	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A7768	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A7769	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A7770	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A7771	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
KAS-ECC-SSC Sp800-56Ar3	A7772	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A7773	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A7774	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A7775	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A7776	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A7777	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A7778	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A7779	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
KAS-ECC-SSC Sp800-56Ar3	A7981	Domain Parameter Generation Methods - P-384 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDA HKDF SP800-56Cr2	A7928	Fixed Info Pattern - uPartyInfo||vPartyInfo Fixed Info Encoding - concatenation Derived Key Length - 128, 192, 256 Shared Secret Length - Shared Secret Length: 256, 384, 528 HMAC Algorithm - SHA2-256, SHA2-384, SHA2-512 Perform Multiple Expansion Tests - No Uses Hybrid Shared Secret - No	SP 800-56C Rev. 2
KDA HKDF SP800-56Cr2	A7982	Fixed Info Pattern - uPartyInfo||vPartyInfo Fixed Info Encoding - concatenation Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-8192 Increment 8 HMAC Algorithm - SHA2-256, SHA2-384, SHA2-512 Perform Multiple Expansion Tests - No Uses Hybrid Shared Secret - No	SP 800-56C Rev. 2
KDF SP800-108	A4199	KDF Mode - Counter MAC Mode - HMAC-SHA2-256, HMAC-SHA2-384 Supported Lengths - Supported Lengths: 256, Supported Lengths: 384 Fixed Data Order - Before Fixed Data Counter Length - 32 Supports Empty IV - No Custom Key In Length - 0	SP 800-108 Rev. 1
KDF SP800-108	A7928	KDF Mode - Counter MAC Mode - HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 Supported Lengths - Supported Lengths: 128, 192, 256 Fixed Data Order - Before Fixed Data Counter Length - 32 Supports Empty IV - No Custom Key In Length - 256, 384, 528	SP 800-108 Rev. 1
KTS-IFC	A7929	Function - keyPairGen IUT ID - 0123456789abcdef Modulo - 2048	SP 800-56B Rev. 2

Algorithm	CAVP Cert	Properties	Reference
		Key Generation Methods - rsakpg1-basic, rsakpg1-prime-factor Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Hash Algorithms - SHA-1, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - literal[] Associated Data Encoding - concatenation Key Length - 128	
KTS-IFC	A7930	Function - keyPairGen IUT ID - 0123456789abcdef Modulo - 2048 Key Generation Methods - rsakpg1-basic, rsakpg1-prime-factor Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Hash Algorithms - SHA-1, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - literal[] Associated Data Encoding - concatenation Key Length - 128	SP 800-56B Rev. 2
KTS-IFC	A7931	Function - keyPairGen IUT ID - 0123456789abcdef Modulo - 2048 Key Generation Methods - rsakpg1-basic, rsakpg1-prime-factor Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Hash Algorithms - SHA-1, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - literal[]	SP 800-56B Rev. 2

Algorithm	CAVP Cert	Properties	Reference
		Associated Data Encoding - concatenation Key Length - 128	
KTS-IFC	A7932	Function - keyPairGen IUT ID - 0123456789abcdef Modulo - 2048 Key Generation Methods - rsakpg1-basic, rsakpg1-prime-factor Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Hash Algorithms - SHA-1, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - literal[] Associated Data Encoding - concatenation Key Length - 128	SP 800-56B Rev. 2
KTS-IFC	A7933	Function - keyPairGen IUT ID - 0123456789abcdef Modulo - 2048 Key Generation Methods - rsakpg1-basic, rsakpg1-prime-factor Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Hash Algorithms - SHA-1, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - literal[] Associated Data Encoding - concatenation Key Length - 128	SP 800-56B Rev. 2
KTS-IFC	A7934	Function - keyPairGen IUT ID - 0123456789abcdef Modulo - 2048 Key Generation Methods - rsakpg1-basic, rsakpg1-prime-factor Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method -	SP 800-56B Rev. 2

Algorithm	CAVP Cert	Properties	Reference
		Hash Algorithms - SHA-1, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - literal[] Associated Data Encoding - concatenation Key Length - 128	
KTS-IFC	A7935	Function - keyPairGen IUT ID - 0123456789abcdef Modulo - 2048 Key Generation Methods - rsakpg1-basic, rsakpg1-prime-factor Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Hash Algorithms - SHA-1, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - literal[] Associated Data Encoding - concatenation Key Length - 128	SP 800-56B Rev. 2
KTS-IFC	A7936	Function - keyPairGen IUT ID - 0123456789abcdef Modulo - 2048 Key Generation Methods - rsakpg1-basic, rsakpg1-prime-factor Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Hash Algorithms - SHA-1, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - literal[] Associated Data Encoding - concatenation Key Length - 128	SP 800-56B Rev. 2
KTS-IFC	A7937	Function - keyPairGen IUT ID - 0123456789abcdef Modulo - 2048 Key Generation Methods - rsakpg1-basic, rsakpg1-prime-factor Fixed Public Exponent - 010001	SP 800-56B Rev. 2

Algorithm	CAVP Cert	Properties	Reference
		Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Hash Algorithms - SHA-1, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - literal[] Associated Data Encoding - concatenation Key Length - 128	
KTS-IFC	A7938	Function - keyPairGen IUT ID - 0123456789abcdef Modulo - 2048 Key Generation Methods - rsakpg1-basic, rsakpg1-prime-factor Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Hash Algorithms - SHA-1, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - literal[] Associated Data Encoding - concatenation Key Length - 128	SP 800-56B Rev. 2
KTS-IFC	A7939	Function - keyPairGen IUT ID - 0123456789abcdef Modulo - 2048 Key Generation Methods - rsakpg1-basic, rsakpg1-prime-factor Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Hash Algorithms - SHA-1, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - literal[] Associated Data Encoding - concatenation Key Length - 128	SP 800-56B Rev. 2
KTS-IFC	A7940	Function - keyPairGen IUT ID - 0123456789abcdef	SP 800-56B Rev. 2

Algorithm	CAVP Cert	Properties	Reference
		Modulo - 2048 Key Generation Methods - rsakpg1-basic, rsakpg1-prime-factor Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Hash Algorithms - SHA-1, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - literal[] Associated Data Encoding - concatenation Key Length - 128	
KTS-IFC	A7941	Function - keyPairGen IUT ID - 0123456789abcdef Modulo - 2048 Key Generation Methods - rsakpg1-basic, rsakpg1-prime-factor Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Hash Algorithms - SHA-1, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - literal[] Associated Data Encoding - concatenation Key Length - 128	SP 800-56B Rev. 2
KTS-IFC	A7942	Function - keyPairGen IUT ID - 0123456789abcdef Modulo - 2048 Key Generation Methods - rsakpg1-basic, rsakpg1-prime-factor Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Hash Algorithms - SHA-1, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - literal[]	SP 800-56B Rev. 2

Algorithm	CAVP Cert	Properties	Reference
		Associated Data Encoding - concatenation Key Length - 128	
KTS-IFC	A7943	Function - keyPairGen IUT ID - 0123456789abcdef Modulo - 2048 Key Generation Methods - rsakpg1-basic, rsakpg1-prime-factor Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Hash Algorithms - SHA-1, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - literal[] Associated Data Encoding - concatenation Key Length - 128	SP 800-56B Rev. 2
KTS-IFC	A7961	Function - keyPairGen IUT ID - 0123456789abcdef Modulo - 2048 Key Generation Methods - rsakpg1-basic, rsakpg1-prime-factor Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - responder Key Transport Method - Hash Algorithms - SHA-1, SHA2-256, SHA2-384, SHA2-512 Supports Null Associated Data - Yes Associated Data Pattern - literal[] Associated Data Encoding - concatenation Key Length - 128	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7929	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7930	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2

Algorithm	CAVP Cert	Properties	Reference
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7931	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7932	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7933	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7934	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7935	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7936	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7937	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7938	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7939	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7940	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2

Algorithm	CAVP Cert	Properties	Reference
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7941	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7942	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7943	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7944	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7945	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7946	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7947	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7948	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7949	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7950	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2

Algorithm	CAVP Cert	Properties	Reference
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7951	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7952	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7953	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7954	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7955	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7956	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7957	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7958	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7959	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2
RSA Decryption Primitive Sp800-56Br2 (CVL)	A7961	Modulo - 2048, 3072, 4096 Key Format - Standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	SP 800-56B Rev. 2

Algorithm	CAVP Cert	Properties	Reference
RSA KeyGen (FIPS186-5)	A7984	Key Generation Mode - probable Modulo - 2048 p mod 8 - 0 Primality Tests - 2pow100 q mod 8 - 0 Fixed Public Exponent - 010001 Info Generated By Server - Yes Private Key Format - standard Public Exponent Mode - fixed	FIPS 186-5
RSA Signature Primitive (CVL)	A7929	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7930	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7931	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7932	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7933	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7934	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7935	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7936	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
RSA Signature Primitive (CVL)	A7937	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7938	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7939	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7940	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7941	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7942	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7943	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7944	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7945	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7946	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
RSA Signature Primitive (CVL)	A7947	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7948	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7949	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7950	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7951	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7952	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7953	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7954	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7955	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7956	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
RSA Signature Primitive (CVL)	A7957	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7958	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7959	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA Signature Primitive (CVL)	A7961	Modulo - 2048, 3072, 4096 Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-4
SHA2-256	A7762	Message Length - Message Length: 8-8192 Increment 8	FIPS 180-4
SHA2-256	A7781	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A7979	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A7762	Message Length - Message Length: 8-8192 Increment 8	FIPS 180-4
SHA2-384	A7781	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A7979	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A6566	Message Length - Message Length: 8-65528 Increment 8	FIPS 180-4
SHA2-512	A7762	Message Length - Message Length: 8-8192 Increment 8	FIPS 180-4
SHA2-512	A7979	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
Symmetric and Asymmetric Cryptographic Key Generation (CKG)	Key type:Symmetric and Asymmetric	N/A	SP800-133r2 section 4, IG D.H additional comment 2, Direct DRBG output

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
HSM AES-GCM with external IV	Encryption/decryption (non-approved due to not being CAVP tested and due to the use of an externally generated IV)

Table 6: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
RSA KeyGen	AsymKeyPair-KeyGen CKG	RSA key pair generation		RSA KeyGen (FIPS186-5): (A7984) Symmetric and Asymmetric Cryptographic Key Generation (CKG): () Key type: Symmetric and Asymmetric
HSM RSA key decapsulation (KTS)	KTS-Decap	RSA key decapsulation	Standard:SP 800-56Br2 IG D.G:approved or allowed method from IG D.G Key confirmation:no Caveat:Key establishment methodology provides 112 bits of security strength	KTS-IFC: (A7929, A7930, A7931, A7932, A7933, A7934, A7935, A7936, A7937, A7938, A7939, A7940, A7941, A7942, A7943, A7961) SHA2-256: (A7762) SHA2-384: (A7762) SHA2-512: (A7762)

Name	Type	Description	Properties	Algorithms
HSM random number generation	DRBG	Random number generation		HMAC DRBG: (A6566) HMAC-SHA2-512: (A6566) SHA2-512: (A6566)
HSP random number generation	DRBG	Random number generation		HMAC DRBG: (A6566) HMAC-SHA2-512: (A6566) SHA2-512: (A6566)
HSP Entropy Source	ENT-ESV	Entropy source		
HSM Entropy Source	ENT-ESV	Entropy source		
HSM AES-KWP unwrapping (KTS)	KTS-Unwrap	AES-KWP unwrapping	Standard:SP 800-38F IG D.G:approved or allowed method from IG D.G Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-KWP: (A7927) AES-ECB: (A7927)
HSP AES-KWP wrapping (KTS)	KTS-Wrap	AES-KWP wrapping	Standard:SP 800-38F IG D.G:approved or allowed method from IG D.G Caveat:Key establishment methodology provides 256 bits of security strength	AES-KWP: (A7980) AES-ECB: (A4199)
HSP AES-KWP unwrapping (KTS)	KTS-Unwrap	AES-KWP unwrapping	Standard:SP 800-38F IG D.G:approved or allowed method from IG D.G Caveat:Key establishment methodology	AES-KWP: (A7980) AES-ECB: (A4199)

Name	Type	Description	Properties	Algorithms
			provides 256 bits of security strength	
HSP AES-GCM encryption	BC-AuthEncrypt	Symmetric encryption		AES-GCM: (A7984) AES-ECB: (A4199)
HSP AES-GCM decryption	BC-AuthDecrypt	Symmetric decryption		AES-GCM: (A7984) AES-ECB: (A4199)
HSM ECDSA KeyGen	AsymKeyPair-KeyGen CKG	Key pair generation		ECDSA KeyGen (FIPS186-5): (A7764, A7765, A7766, A7767, A7768, A7769, A7770, A7771, A7772, A7773, A7774, A7775, A7776, A7777, A7778, A7779) Symmetric and Asymmetric Cryptographic Key Generation (CKG): () Key type: Symmetric and Asymmetric
HSP ECDH KeyGen	AsymKeyPair-KeyGen CKG	Key pair generation		ECDSA KeyGen (FIPS186-5): (A7977) Symmetric and Asymmetric Cryptographic Key Generation (CKG): () Key type: Symmetric and Asymmetric
HSM ECDSA SigGen component	DigSig-SigGen	Signature generation component		ECDSA SigGen (FIPS186-5): (A7764, A7765, A7766, A7767, A7768, A7769, A7770, A7771, A7772, A7773,

Name	Type	Description	Properties	Algorithms
				A7774, A7775, A7776, A7777, A7778, A7779)
HSP ECDSA SigGen for DICE attestation	DigSig-SigGen	Signature generation		ECDSA SigGen (FIPS186-5): (A7977, A7978) SHA2-384: (A7781)
HSP ECDSA SigVer	DigSig-SigVer	Signature verification		ECDSA SigVer (FIPS186-5): (A7976, A7977, A7978) SHA2-384: (A7781)
HSM ECDH shared secret computation	KAS-SSC	ECDH shared secret computation		KAS-ECC-SSC Sp800-56Ar3: (A7764, A7765, A7766, A7767, A7768, A7769, A7770, A7771, A7772, A7773, A7774, A7775, A7776, A7777, A7778, A7779)
HSP ECDH shared secret computation	KAS-SSC	ECDH shared secret computation		KAS-ECC-SSC Sp800-56Ar3: (A7981)
HSM RSA signature generation component	DigSig-SigGen	Signature generation		RSA Signature Primitive: (A7929, A7930, A7931, A7932, A7933, A7934, A7935, A7936, A7937, A7938, A7939, A7940, A7941, A7942, A7943, A7944, A7945, A7946, A7947, A7948, A7949, A7950, A7951, A7952, A7953, A7954, A7955, A7956, A7957, A7958, A7959, A7961)

Name	Type	Description	Properties	Algorithms
HSM RSA decryption component	KTS-Unwrap	RSA decryption component		RSA Decryption Primitive Sp800-56Br2: (A7929, A7930, A7931, A7932, A7933, A7934, A7935, A7936, A7937, A7938, A7939, A7940, A7941, A7942, A7943, A7944, A7945, A7946, A7947, A7948, A7949, A7950, A7951, A7952, A7953, A7954, A7955, A7956, A7957, A7958, A7959, A7961)
HSM HKDF	KAS-56CKDF	HMAC-based key derivation function		SHA2-256: (A7762) SHA2-384: (A7762) SHA2-512: (A7762) KDA HKDF SP800-56Cr2: (A7928) HMAC-SHA2-256: (A7928) HMAC-SHA2-384: (A7928) HMAC-SHA2-512: (A7928)
HSP HKDF	KAS-56CKDF	HMAC-based key derivation function		KDA HKDF SP800-56Cr2: (A7982) HMAC-SHA2-256: (A7983) HMAC-SHA2-384: (A7983) HMAC-SHA2-512: (A7983) SHA2-256: (A7979) SHA2-384: (A7979) SHA2-512: (A7979)
HSM KBKDF	KBKDF	Key-based key derivation function		SHA2-256: (A7762) SHA2-384: (A7762) SHA2-512: (A7762) KDF SP800-108:

Name	Type	Description	Properties	Algorithms
				(A7928) HMAC-SHA2-256: (A7928) HMAC-SHA2-384: (A7928) HMAC-SHA2-512: (A7928)
HSP KBKDF	KBKDF	Key-based key derivation function		KDF SP800-108: (A4199) HMAC-SHA2-256: (A4199) HMAC-SHA2-384: (A4199) SHA2-256: (A7781) SHA2-384: (A7781)
HSM SHA	SHA	Hash function		SHA2-256: (A7762) SHA2-384: (A7762) SHA2-512: (A7762)
HSM HMAC	MAC	Message authentication code		SHA2-256: (A7762) SHA2-384: (A7762) SHA2-512: (A7762) HMAC-SHA2-256: (A7928) HMAC-SHA2-384: (A7928) HMAC-SHA2-512: (A7928)
HSM AES-XTS decryption	BC-UnAuthDecrypt	Symmetric decryption		AES-XTS Testing Revision 2.0: (A7760, A7761) AES-ECB: (A6565)
HSM AES-XTS encryption	BC-UnAuthEncrypt	Symmetric encryption		AES-XTS Testing Revision 2.0: (A7760, A7761) AES-ECB: (A6565)
HSM AES-CBC encryption	BC-UnAuthEncrypt	Symmetric encryption		AES-CBC: (A7763)
HSM AES-CBC decryption	BC-UnAuthDecrypt	Symmetric decryption		AES-CBC: (A7763)
HSM AES-CBC decryption + HSM HMAC	BC-UnAuthDecrypt MAC	Symmetric decryption, HMAC		AES-CBC: (A7763) SHA2-256: (A7762) SHA2-384: (A7762) SHA2-512: (A7762)

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-256: (A7928) HMAC-SHA2-384: (A7928) HMAC-SHA2-512: (A7928)
HSP DICE key derivation	KBKDF	Asymmetric key derivation		KDF SP800-108: (A4199) HMAC-SHA2-256: (A4199) HMAC-SHA2-384: (A4199) SHA2-256: (A7781) SHA2-384: (A7781)
HSM AES Key Generation	CKG	Symmetric key generation		Symmetric and Asymmetric Cryptographic Key Generation (CKG): () HMAC DRBG: (A6566) HMAC-SHA2-512: (A6566) SHA2-512: (A6566)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

AES XTS:

AES-XTS is only approved for and shall only be used for storage purposes. Per IG C.I, AES-XTS Key_1 and/or Key_2, when entered into the module by the operator, shall be generated and/or established independently of each other according to the rules for component symmetric keys from NIST SP 800-133rev2, Sec. 6.3 for an approved use of AES-XTS.

The module implements a check that ensures the length of a single data unit encrypted with the XTS-AES does not exceed 2^{20} AES blocks, that is, 16MB of data.

The module implements a check that ensures, before performing any cryptographic operation, the two AES keys used in AES XTS mode are not identical.

AES-GCM IV (related to the HSP AES-GCM encryption and HSP AES-GCM decryption security functions):

The module generates GCM IV in compliance with scenario 5 of IG C.H. The IV length is 96 bits (32-bit fixed field and 64-bit invocation field), and the IV value is deterministic in compliance with the SPDM protocol version 1.3.0. The design of the SPDM protocol implicitly ensures that the counter (the SPDM sequence number of the IV) does not exhaust the maximum number of possible values for a given SPDM session key. In case of power loss, the IV and key are freshly generated from derived session keys and random nonces, through

a new SPDM session establishment. The use of AES-GCM within this protocol is defined in the specification DSP0274. The module's GCM implementation with an IV generated outside the GCM implementation used as part of an approved mechanism is limited to the discussed SPDM protocol.

RSA Signature Generation Component:

The module's RSA signature generation component implementations were CAVP tested with moduli sizes 2048, 3072, and 4096 bits. The module only supports these moduli sizes. The RSA SigGen (CVL) shall only be used within the context of a FIPS 186-5 signature generation.

RSA Decryption Component:

The module's RSA decryption component implementations were CAVP tested with moduli sizes 2048, 3072, and 4096 bits. The module only supports these moduli sizes. The RSA Decryption Primitive (CVL) shall only be used within the context of a SP 800-56Brev2 KTS.

RSA Key Generation:

The module's RSA key generation implementation was CAVP tested with moduli size 2048 bits. This modulus size is allowed by FIPS 140-3 IG C.F. The number of Miller-Rabin tests is compliant with Table B.1 of FIPS 186-5.

SP 800-56B Rev.2 Assurances:

The module offers KTS-OAEP compliant with SP 800-56BRev2 and IG D.G. The module only uses internally generated RSA keys for KTS-OAEP, which meet the assurances required by the key pair owner defined in section 6.4.1 of SP 800-56BRev2.

The module does not accept public keys from outside entities. Therefore, the assurances defined in section 6.4.2 of SP 800-56BRev2 are not applicable.

ECDSA Signature Generation Component:

The ECDSA SigGen (CVL) shall only be used within the context of a FIPS 186-5 signature generation.

SP 800-56ARev3 Assurances:

The module offers ECDH shared secret computation (of the Diffie-Hellman variety, not the MQV variety) compliant with SP 800-56ARev3 and meeting IG D.F scenario 2 path (1). To meet the required assurances listed in section 5.6 of SP 800-56Arev3, the following steps shall be performed.

1. The entity using the module must use the module's service for generating ECDH ephemeral keys. This meets the assurances required by the key pair owner defined in section 5.6.2.1 of SP 800-56ARev3.

2. As part of the module's shared secret computation implementation, the module internally performs the public key validation on the peer's public key passed in as input to the function. This meets the public key validity assurance required by section 5.6.2.2.2 of SP 800-56ARev3.

3. The module does not support static keys; therefore, the "assurance of peer's possession of private key" is not applicable.

Curves used in KAS-ECC-SSC:

The module supports KAS-ECC-SSC with P-256, P-384, and P-521. The bit lengths "N" of the private key and the maximum security strength "s" supported by these curves are:

- For P-256, N is 256 bits and s is 128 bits
- For P-384, N is 384 bits and s is 192 bits

- For P-521, N is 521 bits and s is 256 bits

2.8 RBG and Entropy

Cert Number	Vendor Name
E166	Microsoft Corporation

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
M1244265-004 B0 Entropy Source	Physical	Microsoft M1244265-004 B0 (TRNG HSM); Microsoft M1244265-004 B0 (TRNG HSP)	1 bit	0.5 bits	None

Table 9: Entropy Sources

The module implements two SP 800-90ARev1-compliant Deterministic Random Bit Generators (DRBGs), specifically HMAC DRBG using HMAC-SHA2-512 which provides 256 bits of security strength. The two DRBG implementations are identical. The DRBGs do not support prediction resistance.

The module includes two instances of the M1244265-004 B0 Entropy Source (ESV certificate E166). Each entropy source instance seeds one HMAC_DRBG instance and provides an entropy rate of 0.5 bit/bit.

During instantiation and reseeding, each DRBG performs one GetEntropy() call to receive 1,024 bits of entropy input containing 512 bits of entropy.

The following is the link to the Public Use Document of the entropy source:

https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/entropy/E166_PublicUse.pdf

2.9 Key Generation

The module implements Cryptographic Key Generation (CKG, vendor affirmed), compliant with SP 800-133r2. When random values are required, they are obtained from the SP 800-90Ar1 approved DRBG of type HMAC_DRBG, compliant with section 4 of SP 800-133r2. This method does not use the value V as described in Additional Comment 2 of FIPS 140-3 IG D.H.

The following methods are implemented:

- Symmetric key generation for AES,
- RSA key pair generation,
- ECC key pair generation

Intermediate key generation values are not output from the module and are explicitly zeroized before the completion of the algorithm.

Additionally, the module implements the following key derivation methods, per SP 800-133r2, section 6.2:

- KBKDF,

- HKDF

All the CAVP certificates for these algorithms can be found in the Approved Algorithms table in Section 2.5 of this Security Policy.

2.10 Key Establishment

The module implements key establishment methods as listed in the Security Function Implementations table in Section 2.6 of this Security Policy.

The module implements KAS-ECC-SSC with curves P-256, P-384, and P-521.

The module implements KTS-IFC (RSA-OAEP) with a 2048-bit modulus, which was also the modulus size used during testing. RSA keys are generated using the rsakpg1-basic method. The module performs only un-encapsulation and does not perform key confirmation as part of key transport. Required assurances are performed by the module in accordance with section 6.4 of SP 800-56Br2.

The module supports a hybrid key transport scheme as specified in section 9.3 of SP 800-56BRev2. In this scheme, KTS-IFC is used to un-encapsulate an AES-KWP key, which in turn unwraps a second key used to perform HSM services.

2.11 Industry Protocols

The module uses AES-GCM in the context of the SPDM protocol. No part of the SPDM protocol, other than the AES-GCM, has been tested by the CAVP or CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
PCIe Gen 5	Data Input Data Output Control Input Status Output	HSM input data, output data, control input, status output through logical FW APIs
I2C	Data Input Data Output Control Input Status Output	HSP input data, output data, control input, status output through logical FW APIs
Quad SPI	Data Input Data Output	HSP input data, output data through logical FW APIs
UART	Status Output	Status output in registers
Physical power rails	Power	N/A

Table 10: Ports and Interfaces

The module does not implement a control output interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
ID and PIN	Identity Based Authentication used to assume the DDI role	128 bit ID and PIN based authentication	The probability of successfully guessing the correct PIN in one random attempt is 1 in 2^128.	Due to delays enforced by the module after failed authentication attempts, the maximum number of wrong PIN attempts in a minute is 1000. This means there is a probability of 1000/(2^128) of randomly guessing the correct PIN in a minute, which is approximately 1 in 2^118.
Challenge-response Protocol	Identity Based Authentication used to assume the Crypto Officer role	HSP ECDSA SigVer	Since the ECC curve used in this mechanism is P-384, the probability of successfully and randomly guessing a signature is 1 in 2^192.	The maximum bandwidth of the interface used to physically transmit the signature is 3.2 Mbps or 192 * 10^6 bits per minute. The size of the signature (r,s) is 384*2 = 768 bits. Conservatively accounting for only the size of the signature, that corresponds to 192 * 10^6 / 768 = 250000 signatures that can be transmitted in a minute. Conservatively assuming the signature verification in the module is instantaneous, the maximum probability of randomly guessing a correct signature in a minute is the maximum number of signature verifications in a minute divided by the strength of the signature algorithm, or 250000/(2^192) which is approximately 1 in 2^174.
Signed token	Identity Based Authentication used to assume the Crypto Officer role	HSP ECDSA SigVer	Since the ECC curve used in this mechanism is P-384, the probability of successfully and randomly guessing a signature is 1 in 2^192.	The maximum bandwidth of the interface used to physically transmit the signature is 3.2 Mbps or 192 * 10^6 bits per minute. The size of the signature (r,s) is 384*2 = 768 bits. Conservatively accounting for only the size of the signature, that corresponds to 192 * 10^6 / 768 = 250000 signatures that can be transmitted in a minute. Conservatively assuming

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
				the signature verification in the module is instantaneous, the maximum probability of randomly guessing a correct signature in a minute is the maximum number of signature verifications in a minute divided by the strength of the signature algorithm, or 250000/(2^192) which is approximately 1 in 2^174.

Table 11: Authentication Methods

ID and PIN:

To assume the DDI role (described in the next section), the operator must first establish an ID and PIN through a two-stage process.

First stage: The module and operator exchange ECC public keys, and the module sends a nonce to the operator. Both parties then perform ECDH and derive AES and HMAC keys using HKDF, incorporating the nonce. The operator selects an ID and PIN and encrypts each separately with AES-CBC using an operator-chosen IV, producing two ciphertexts. The operator then computes an HMAC over the concatenation of the encrypted ID, encrypted PIN, AES-CBC IV, and nonce. The operator sends all four values along with the HMAC tag to the module. The module verifies the HMAC tag and, if verification succeeds, decrypts and stores the ID and PIN. This ID identifies the operator.

Second stage: The module and operator again exchange ECC public keys — though the module uses a different public key this time — and the module sends a new nonce. Both parties again perform ECDH and derive AES and HMAC keys using HKDF with the new nonce. The operator re-encrypts the same ID and PIN separately with AES-CBC using a new operator-chosen IV, then computes an HMAC over the concatenation of the encrypted ID, encrypted PIN, AES-CBC IV, and nonce. The operator sends all four values along with the HMAC tag to the module. The module verifies the HMAC tag and, if verification succeeds, decrypts the ID and PIN and checks them against the values stored during the first pass.

If both values match, the module issues a session ID to the operator. This session ID must accompany every subsequent operator request for services allocated to the DDI role.

Challenge-response:

The module issues a random challenge value to the operator, who signs it and returns the signature alongside the requested service call. The module verifies the signature against a public key that identifies the operator. This challenge-response exchange is required each time the operator invokes a service that uses this authentication mechanism.

Signed token:

The operator submits a signed token to the module along with the requested service call. The module verifies the token's signature against a public key that identifies the operator. This verification is required each time the operator invokes a service that uses this authentication mechanism.

Upon power-off, all previous authentications are cleared and the operator must re-authenticate.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	CO	Challenge-response Protocol Signed token
DDI Role	Identity	User	ID and PIN
User Role	Role	User	None

Table 12: Roles

The module concurrently supports one operator connected to the I2C interface (who can be in the Crypto Officer role or User role) and up to 64 operators in the DDI role. Alternatively, the module concurrently supports one operator connected to the I2C interface (who can be in the Crypto Officer role or User role) and up to 64 operators in the User role connected through the PCIe Gen 5 interface.

The services of the Crypto Officer role are accessible only via the I2C interface; the services of the DDI role are accessible only via the PCIe Gen 5 interface. In this way, two concurrent operators in the CO and DDI roles will be unable to access the services of the other operator due to them connecting to the module through these different physical interfaces. This also means that role changes between the DDI role and Crypto Officer role are not possible.

An unauthenticated operator cannot access services of the DDI role or Crypto Officer role, because the module always requires authentication data to access these services for each service invocation.

An operator who has assumed the unauthenticated User role may change roles to the DDI role only by performing the necessary authentication as described in Section 4.1 of this Security Policy. Similarly, an operator who has assumed the unauthenticated User role may change roles to the Crypto Officer role only by performing the necessary authentication as described in Section 4.1 of this Security Policy.

An operator who has assumed the DDI role may change roles to the unauthenticated User role by invoking the "Close session (HSM)" service. This clears the DDI role authentication.

4.3 Approved Services

All approved services implemented by the module are listed in the table below. The following convention is used to specify access rights to SSPs:

Generate (G): The module generates or derives the SSP.

Read (R): The SSP is read from the module (e.g. the SSP is output).

Write (W): The SSP is updated, imported, or written to the module.

Execute (E): The module uses the SSP in performing a cryptographic operation.

Zeroize (Z): The module zeroizes the SSP.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Get API revision (HSM)	Provides DDI API version information	None	None	Minimum and maximum revision of the API supported	None	User Role DDI Role

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
				by the DDI interface		
Get device info (HSM)	Provides device information	None	None	Device kind (whether the module is a chip or not), number of key tables available to HSM services	None	User Role DDI Role
Delete key (HSM)	Delete a key from key storage	fips_approved is 1	Key ID	None	None	DDI Role
Open key (HSM)	Get the ID of a key from its name	fips_approved is 1	Key name	Key ID, key type, public key (if available)	None	DDI Role - HSM ECC public key: R - HSM RSA public key: R
Attest key (HSM)	Generate attestation report for key	fips_approved is 1	Key ID, report data to be included in the report	Attestation report	HSM ECDSA SigGen component HSM SHA	DDI Role - HSP ECDSA private key (DICE): E
Get collateral (HSM)	Provides certificates used internally by the module	fips_approved is 1	Collateral type, certificate Id	Certificates	None	DDI Role
Import RSA-encapsulated key (HSM)	Unencapsulate a key using RSA-OAEP and AES-KWP	fips_approved is 1	Unwrapping key ID, wrapped key	Key ID, public key	HSM RSA key decapsulation (KTS) HSM AES-KWP unwrapping (KTS)	DDI Role - RSA Unwrapping key: E - HSM AES Key: W,E
Get RSA unwrapping key ID (HSM)	Provides ID for RSA unwrapping key, and the corresponding	fips_approved is 1	None	Key ID, corresponding wrapping key	RSA KeyGen HSP AES-KWP	DDI Role - RSA Wrapping key: G,R - RSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	RSA wrapping key				unwrapping (KTS)	Unwrapping key: G - HSP AES Key: E
RSA signature generation (HSM)	Perform an RSA signature generation component operation	fips_approved is 1	RSA key ID, data	Signature	HSM RSA signature generation component	DDI Role - HSM RSA private key: E
RSA decryption component (HSM)	Perform an RSA decryption component operation	fips_approved is 1	RSA key ID, ciphertext	Plaintext	HSM RSA decryption component	DDI Role - HSM RSA private key: E
ECC KeyGen (HSM)	Generate an ECC key pair	fips_approved is 1	Curve	Key ID for private key; public key	HSM ECDSA KeyGen	DDI Role - HSM ECC public key: G,R - HSM ECC private key: G
ECDSA SigGen (HSM)	Perform an ECDSA signature generation component operation	fips_approved is 1	Key ID for private key, data	Signature	HSM ECDSA SigGen component	DDI Role - HSM ECC private key: E
ECDH SSC (HSM)	ECDH shared secret computation	fips_approved is 1	Key ID for private key; public key	Key ID for ECDH secret	HSM ECDH shared secret computation	DDI Role - HSM ECC public key: W,E - HSM ECC private key: E - HSM ECDH Secret: G
Generate AES key (HSM)	Symmetric key generation	fips_approved is 1	Key length	Key ID	HSM AES Key Generation	DDI Role - HSM AES Key: G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
AES-CBC encryption (HSM)	AES-CBC encryption	fips_approved is 1	Key ID, plaintext, IV	Ciphertext	HSM AES-CBC encryption	DDI Role - HSM AES Key: E
AES-CBC decryption (HSM)	AES-CBC decryption	fips_approved is 1	Key ID, ciphertext, IV	Plaintext	HSM AES-CBC decryption	DDI Role - HSM AES Key: E
AES-XTS encryption (HSM)	AES-XTS encryption	fips_approved is 1	Key ID, plaintext, tweak	Ciphertext	HSM AES-XTS encryption	DDI Role - HSM AES Key: E
AES-XTS decryption (HSM)	AES-XTS decryption	fips_approved is 1	Key ID, ciphertext, tweak	Plaintext	HSM AES-XTS decryption	DDI Role - HSM AES Key: E
HKDF (HSM)	Derive a key via HKDF	fips_approved is 1	Key ID of ECDH shared secret, salt, info, derived key length	Key ID of derived key	HSM HKDF	DDI Role - HSM AES Key: G - HSM ECDH Secret: E - HSM HMAC key: G
HKDF + KBKDF (HSM)	Derive a key from a shared secret using HKDF, and then perform KBKDF on the derived symmetric key	fips_approved is 1	Key ID of shared secret, other info	Key ID of derived key	HSM HKDF HSM KBKDF	DDI Role - HSM AES Key: G - HSM HMAC key: G - HSM key derivation key: G,E - HSM ECDH Secret: E
HMAC (HSM)	Message authentication code	fips_approved is 1	Key ID, message	MAC tag	HSM HMAC	DDI Role - HSM HMAC key: E
Get ECC public key for establishing PIN (HSM)	Provides ECC public key - this is needed as part of the	fips_approved is 1	None	ECC public key	HSM random number generation HSM	User Role - HSM ECC public key: R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	authentication mechanism				Entropy Source HSM ECDSA KeyGen	
Establish PIN (HSM)	Establishes a PIN	fips_approved is 1	Encrypted PIN, ECC public key	None	HSM ECDH shared secret computation HSM HKDF HSM AES-CBC decryption + HSM HMAC	User Role - HSM Operator PIN: W - HSM AES Key: G,E - HSM HMAC key: G,E - HSM ECC public key: W,E - HSM ECDH Secret: G,E - HSM ECC private key: E
Get ECC public key for opening session (HSM)	Provides ECC public key - this is needed as part of the authentication mechanism	fips_approved is 1	None	ECC public key	HSM random number generation HSM Entropy Source HSM ECDSA KeyGen	User Role - HSM ECC public key: R
Open session (HSM)	Opens user session - part of the authentication mechanism	fips_approved is 1	Encrypted ID, Encrypted PIN, IV, nonce, HMAC tag, DER encoded public key	Success/failure	HSM ECDH shared secret computation HSM HKDF HSM AES-CBC decryption + HSM HMAC	User Role - HSM Operator PIN: W - HSM AES Key: G,E - HSM HMAC key: G,E - HSM ECC public key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,E - HSM ECDH Secret: G,E - HSM ECC private key: E
Change PIN (HSM)	Changes the PIN	fips_approved is 1	Encrypted PIN, ECC public key	None	HSM ECDH shared secret computation HSM HKDF HSM AES-CBC decryption + HSM HMAC	DDI Role - HSM Operator PIN: W - HSM AES Key: G,E - HSM HMAC key: G,E - HSM ECC public key: W,E - HSM ECDH Secret: G,E - HSM ECC private key: E
Close session (HSM)	Closes user session (change roles from DDI role to the unauthenticated User role)	fips_approved is 1	None	None	None	DDI Role
Fuse zeroization (HSP)	Zeroize fuse secrets by transitioning the module to the RETEST state	None	None	None	None	Crypto Officer - Fuse secrets: Z User Role - Fuse secrets: Z
Firmware update (HSP)	Perform a firmware update	HSP indicator returns "FIPS"	Firmware image	Pass/fail	HSP ECDSA SigVer	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Reset device configuration without SPDM (HSP)	Reset device configuration without using an SPDM session to encrypt data in transit	HSP indicator returns "FIPS"	None	Pass/fail	None	Crypto Officer
Reset device configuration with SPDM (HSP)	Reset device configuration by using SPDM session to encrypt data in transit	HSP indicator returns "FIPS"	ECC public key	ECC public key, Pass/fail	HSP AES-GCM encryption HSP AES-GCM decryption HSP ECDH KeyGen HSP ECDH shared secret computation HSP HKDF	Crypto Officer - HSP ECDH public key: G,R,W,E - HSP ECDH private key: G,E - HSP AES Key: G,E - HSP ECDH Secret: G,E
Device attestation (HSP)	Prove the identity of the module to the operator by signing a nonce	HSP indicator returns "FIPS"	Nonce	Signature, device status	HSP ECDSA SigGen for DICE attestation HSP DICE key derivation HSP KBKDF	User Role - HSP ECDSA private key (DICE): G,E - Fuse secrets: E - HSP key derivation key: G,E Crypto Officer - HSP ECDSA private key (DICE): G,E - Fuse secrets: E - HSP key derivation key: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Access error log (HSP)	Get self-test failures	None	N/A	Error log containing self-test failures	None	User Role Crypto Officer
Show status	Get returned status code from every service	None	None	Status (success/failure)	None	Crypto Officer DDI Role User Role
Get device state (UART status)	Get information on the device state	None	None	Device state	None	Crypto Officer User Role
Show module name and version (HSP)	Return the module name and version information	None	N/A	Module name and version	None	User Role Crypto Officer
On-demand self-tests	Perform pre-operational and power-on conditional algorithm self-tests	None	N/A	Pass/fail	HSM RSA key decapsulation (KTS) HSM random number generation HSP random number generation HSP Entropy Source HSM Entropy Source HSM AES-KWP unwrapping (KTS) HSP AES-KWP wrapping (KTS) HSP AES-KWP	User Role Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					unwrapping (KTS) HSP AES-GCM encryption HSP AES-GCM decryption HSM ECDSA SigGen component HSP ECDSA SigGen for DICE attestation HSP ECDSA SigVer HSM ECDH shared secret computation HSP ECDH shared secret computation HSM RSA signature generation component HSM HKDF HSP HKDF HSM KBKDF HSP KBKDF HSM AES-XTS decryption HSM AES-XTS encryption HSM AES-CBC encryption HSM AES-	

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					CBC decryption	
Power-on reset zeroization	Zeroize SSPs via power-on reset	None	None	None	None	User Role - RSA Wrapping key: Z - RSA Unwrapping key: Z - HSM AES Key: Z - HSP AES Key: Z - HSM Entropy Input: Z - HSM DRBG Seed: Z - HSM DRBG Internal State: Z - HSM ECC public key: Z - HSM ECC private key: Z - HSP ECDH private key: Z - HSP ECDH public key: Z - HSM ECDH Secret: Z - HSP ECDH Secret: Z - HSM RSA public key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - HSM RSA private key: Z - HSM Operator PIN: Z - Intermediate key generation value: Z - HSM HMAC key: Z - HSM key derivation key: Z - HSP key derivation key: Z - HSP Entropy Input: Z - HSP DRBG Seed: Z - HSP DRBG Internal State: Z Crypto Officer - RSA Wrapping key: Z - RSA Unwrapping key: Z - HSM AES Key: Z - HSP AES Key: Z - HSM Entropy

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Input: Z - HSM DRBG Seed: Z - HSM DRBG Internal State: Z - HSM ECC public key: Z - HSM ECC private key: Z - HSP ECDH private key: Z - HSP ECDH public key: Z - HSM ECDH Secret: Z - HSP ECDH Secret: Z - HSM RSA public key: Z - HSM RSA private key: Z - HSM Operator PIN: Z - Intermediate key generation value: Z - HSM HMAC key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- HSM key derivation key: Z - HSP key derivation key: Z - HSP Entropy Input: Z - HSP DRBG Seed: Z - HSP DRBG Internal State: Z

Table 13: Approved Services

Every service output contains status information on the success/failure of the requested service.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
AES-GCM (HSM)	Encryption and decryption	HSM AES-GCM with external IV	DDI Role

Table 14: Non-Approved Services

4.5 External Software/Firmware Loaded

The module performs the loading of external firmware in two scenarios:

1. Every time the module starts up, firmware stored outside the module boundary is transferred into the module, as explained in FIPS 140-3 IG 10.3.F additional comment 3 part a. This is the introduction of additional firmware components, not the updating of existing firmware components.

2. The module offers a firmware update service which is invocable by the Crypto Officer operator. This service updates existing firmware components, but does not introduce additional firmware components.

In either case, the module verifies the external firmware using ECDSA P-384 with SHA-384 before the external firmware is executed. All the non-ROM firmware is loaded externally on start-up. The firmware update service allows for updates to the non-ROM firmware. All data output through the data output interface is inhibited while the firmware load test is being performed and until it is completed.

5 Software/Firmware Security

5.1 Integrity Techniques

The module does not perform an integrity test (a firmware load test is performed).

The integrity test is not applied for ROM firmware as the vendor claims the memory technology will not degrade for 10 years after the date of manufacture, in compliance with FIPS 140-3 IG 5.A. The end-of-life procedures described in Section 11.4 of this Security Policy shall be followed before 10 years have elapsed from the date of manufacture.

The module does not provide any services via the HMI, SFMI, HFMI, or HSMI interface that allow the operator to examine the executable code.

5.2 Initiate on Demand

This section is not applicable, as the module does not perform an integrity test.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

The module operates in a limited modifiable operational environment. The module claims physical security at level 3. Therefore, this section is not applicable.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Opaque sealing coat	No actions are required to maintain the physical security of the module	No actions are required to maintain the physical security of the module

Table 15: Mechanisms and Actions Required

7.2 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-35°C +/- 5°C	EFP	Module stops all operations and shuts down
HighTemperature	125°C +/- 5°C	EFP	Module stops all operations and shuts down
LowVoltage	734mV +/- 50mV	EFP	Module stops all operations and shuts down
HighVoltage	923mV +/- 50mV	EFP	Module stops all operations and shuts down

Table 16: EFP/EFT Information

7.3 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-40°C
HighTemperature	125°C

Table 17: Hardness Testing Temperatures

8 Non-Invasive Security

This module does not implement any non-invasive security mechanism and therefore this section is not applicable.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
HSM GSRAM	The global SRAM stores keys for use by the HSM	Dynamic
HSM Fast-path Key Vault	The HSM fast-path key vault stores 256 bit keys exclusively for the HSM AES-GCM and AES-XTS (fast-path)	Dynamic
HSM UPKA SRAM	Internal SRAM for HSM UPKA	Dynamic
HSM RNG Registers	Internal registers used by HSM DRBG	Dynamic
HSP KSU	The key storage unit contains memory that stores keys for use by the HSP	Dynamic
HSP SRAM	The HSP SRAM stores keys for use by the HSP	Dynamic
HSP PKA SRAM	Internal SRAM for HSP PKA	Dynamic
HSP RNG Registers	Internal registers used by HSP DRBG	Dynamic
Fuses	HSP fuse storage	Static

Table 18: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
DDI Import of Non-fast Path Keys	Outside entity	HSM GSRAM	Encrypted	Automated	Electronic	HSM AES-KWP unwrapping (KTS)
DDI Import of Fast Path Keys	Outside entity	HSM Fast-path Key Vault	Encrypted	Automated	Electronic	HSM AES-KWP unwrapping (KTS)
DDI Public Key Export	HSM GSRAM	Outside entity	Plaintext	Automated	Electronic	
DDI Import of AES-KWP Keys	Outside entity	HSM GSRAM	Encrypted	Automated	Electronic	HSM RSA key decapsulation (KTS)
DDI Import of PIN	Outside entity	HSM GSRAM	Encrypted	Automated	Electronic	HSM AES-CBC decryption + HSM HMAC
Import of Public Key into HSP KSU	Outside entity	HSP KSU	Plaintext	Automated	Electronic	

Table 19: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power-on reset	Zeroizes SSPs	The module performs a power-on reset which overwrites SSPs with zeroes or with random data. The availability of the module and responsiveness to operator requests indicates that zeroization was completed.	Power-cycling
Automatic	Automatically zeroized by the module when no longer needed	The module overwrites SSPs with zeroes or with random data. The successful completion of the cryptographic service which generates and zeroizes the SSP indicates that zeroization was completed.	N/A
Fuse zeroization	Zeroizes fuse secrets	The module overwrites fuse secrets with ones. The destruction of the module indicates that zeroization was completed.	Transitioning the module to the RETEST state

Table 20: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
RSA Wrapping key	Sent to the operator who will encrypt SSPs outside the module before importing them into the module	2048 - 112	Public key - PSP	RSA KeyGen		
RSA Unwrapping key	Used in RSA-OAEP key un-encapsulation	2048 - 112	Private key - CSP	RSA KeyGen		HSM RSA key decapsulation (KTS)
HSM AES Key	Used for symmetric encryption and decryption	128, 192, 256 - 128, 192, 256	Symmetric key - CSP	HSM random number generation HSM HKDF HSM KBKDF		HSM AES-KWP unwrapping (KTS) HSM AES-XTS decryption HSM AES-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						XTS encryption HSM AES-CBC encryption HSM AES-CBC decryption HSM AES-CBC decryption + HSM HMAC
HSP AES Key	Used for symmetric encryption and decryption	128, 192, 256 - 128, 192, 256	Symmetric key - CSP	HSP random number generation HSP HKDF		HSP AES-KWP wrapping (KTS) HSP AES-KWP unwrapping (KTS) HSP AES-GCM encryption HSP AES-GCM decryption
HSM Entropy Input	Used to form DRBG seed	1024 - 512	Entropy - CSP	HSM Entropy Source		HSM random number generation
HSM DRBG Seed	Used to instantiate DRBG	888 - 256	DRBG seed - CSP	HSM random number generation		HSM random number generation
HSM DRBG Internal State	Used to generate random numbers	V = 512 bits, Key = 512 bits - 256	DRBG internal state - CSP	HSM random number generation		HSM random number generation
HSP Entropy Input	Used to form DRBG seed	1024 - 512	Entropy - CSP	HSP Entropy Source		HSP random number generation
HSP DRBG Seed	Used to instantiate DRBG	888 - 256	DRBG seed - CSP	HSP random number generation		HSP random number generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
HSP DRBG Internal State	Used to generate random numbers	V = 512 bits, Key = 512 bits - 256	DRBG internal state - CSP	HSP random number generation		HSP random number generation
HSM ECC public key	ECC public key	P-256, P-384, P-521 - 128, 192, 256	Public key - PSP	HSM ECDSA KeyGen		HSM ECDH shared secret computation
HSM ECC private key	ECC private key	P-256, P-384, P-521 - 128, 192, 256	Private key - CSP	HSM ECDSA KeyGen		HSM ECDSA SigGen component
HSP ECDH private key	ECC private key	P-384 - 192	Private key - CSP	HSP ECDH KeyGen		HSP ECDH shared secret computation
HSP ECDH public key	ECC public key	P-384 - 192	Public key - PSP	HSP ECDH KeyGen		HSP ECDH shared secret computation
HSM ECDH Secret	ECDH shared secret	P-256, P-384, P-521 - 128, 192, 256	Shared secret - CSP	HSM ECDH shared secret computation		HSM HKDF
HSP ECDH Secret	ECDH shared secret	P-384 - 192	Shared secret - CSP	HSP ECDH shared secret computation		HSP HKDF
HSM RSA public key	RSA public key	2048, 3072, 4096-bit modulus - 112, 128, 149	Public key - PSP			HSM RSA signature generation component HSM RSA decryption component
HSM RSA private key	RSA private key	2048, 3072, 4096-bit modulus - 112, 128, 149	Private key - CSP			HSM RSA signature generation component HSM RSA

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						decryption component
HSM Operator PIN	Used for operator authenticaton	128 - 128	Authentication PIN - CSP			
Intermediate key generation value	Intermediate value generated during key pair generation	256-2048 - 128-256	Intermediate key generation value - CSP			
HSM HMAC key	Key used for HMAC	256, 384, 512 - 128-256	Symmetric key - CSP	HSM HKDF HSM KBKDF		HSM HMAC
HSM key derivation key	Symmetric key derivation key used in KBKDF	256, 384, 528 - 256	Symmetric key - CSP	HSM HKDF		HSM KBKDF
Fuse secrets	Used by KBKDF	32 - N/A	Key derivation key - CSP			HSP KBKDF
HSP key derivation key	Used by KBKDF	256, 384 - 256	Symmetric key - CSP	HSP KBKDF		HSP KBKDF
HSP ECDSA private key (DICE)	Used by ECDSA SigGen	P-384 - 192	Private key - CSP	HSP DICE key derivation		HSP ECDSA SigGen for DICE attestation

Table 21: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
RSA Wrapping key	DDI Public Key Export	HSP SRAM:Plaintext HSM GSRAM:Plaintext	Until the module is reset	Power-on reset	Intermediate key generation value:Generated from
RSA Unwrapping key		HSP SRAM:Plaintext HSM GSRAM:Plaintext HSM UPKA SRAM:Plaintext	Until the module is reset	Power-on reset	Intermediate key generation value:Generated from
HSM AES Key	DDI Import	HSM GSRAM:Plaintext	Until the module is reset	Power-on reset	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	of Non-fast Path Keys DDI Import of Fast Path Keys DDI Import of AES-KWP Keys	HSM Fast-path Key Vault:Plaintext			
HSP AES Key		HSP KSU:Plaintext	Until the module is reset	Power-on reset	
HSM Entropy Input		HSM RNG Registers:Plaintext	Until the module is reset	Power-on reset	HSM DRBG Seed:Used to generate
HSM DRBG Seed		HSM RNG Registers:Plaintext	Until the module is reset	Power-on reset	HSM Entropy Input:Generated from HSM DRBG Internal State:Used to generate
HSM DRBG Internal State		HSM RNG Registers:Plaintext	Until the module is reset	Power-on reset	HSM DRBG Seed:Generated from
HSP Entropy Input		HSP RNG Registers:Plaintext	Until the module is reset	Power-on reset	HSP DRBG Seed:Used to generate
HSP DRBG Seed		HSP RNG Registers:Plaintext	Until the module is reset	Power-on reset	HSP Entropy Input:Generated from HSP Internal State:Used to generate
HSP DRBG Internal State		HSP RNG Registers:Plaintext	Until the module is reset	Power-on reset	HSP DRBG Seed:Generated from
HSM ECC public key	DDI Import	HSM GSRAM:Plaintext	Until the module is reset	Power-on reset	HSM ECC private key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	of Non-fast Path Keys DDI Public Key Export	HSM UPKA SRAM:Plaintext			HSM ECDH Secret:Used to derive Intermediate key generation value:Generated from
HSM ECC private key	DDI Import of Non-fast Path Keys	HSM GSRAM:Plaintext HSM UPKA SRAM:Plaintext	Until the module is reset	Power-on reset	HSM ECC public key:Paired With HSM ECDH Secret:Used to derive Intermediate key generation value:Generated from
HSP ECDH private key		HSP PKA SRAM:Plaintext HSP KSU:Plaintext	Copy in HSP PKA SRAM: Until key generation is completed. Copy in HSP KSU: Until the module is reset	Power-on reset Automatic	HSP ECDH public key:Paired With HSP ECDH Secret:Used to derive Intermediate key generation value:Generated from
HSP ECDH public key	Import of Public Key into HSP KSU	HSP PKA SRAM:Plaintext HSP KSU:Plaintext	Copy in HSP PKA SRAM: Until key generation is completed. Copy in HSP KSU: Until the module is reset	Power-on reset Automatic	HSP ECDH private key:Paired With HSP ECDH Secret:Used to derive Intermediate key generation value:Generated from
HSM ECDH Secret		HSM GSRAM:Plaintext HSM UPKA SRAM:Plaintext	Until the module is reset	Power-on reset	HSM ECC public key:Derived From HSM ECC private key:Derived From
HSP ECDH Secret		HSP PKA SRAM:Plaintext HSP KSU:Plaintext	Copy in HSP PKA SRAM: Until key generation is completed. Copy in	Power-on reset Automatic	HSP ECDH private key:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			HSP KSU: Until the module is reset		HSP ECDH public key:Derived From
HSM RSA public key	DDI Import of Non-fast Path Keys DDI Public Key Export	HSM GSRAM:Plaintext HSM UPKA SRAM:Plaintext	Until the module is reset	Power-on reset	HSM RSA private key:Paired With
HSM RSA private key	DDI Import of Non-fast Path Keys	HSM GSRAM:Plaintext HSM UPKA SRAM:Plaintext	Until the module is reset	Power-on reset	HSM RSA public key:Paired With
HSM Operator PIN	DDI Import of PIN	HSM GSRAM:Plaintext	Until the module is reset	Power-on reset	
Intermediate key generation value		HSM UPKA SRAM:Plaintext HSP PKA SRAM:Plaintext HSP SRAM:Plaintext	Copy in HSM UPKA SRAM: Until key generation is completed. Copy in HSP PKA SRAM: Until key generation is completed. Copy in HSP KSU: Until the module is reset	Power-on reset Automatic	RSA Wrapping key:Used to generate RSA Unwrapping key:Used to generate HSM ECC public key:Used to generate HSM ECC private key:Used to generate HSP ECDH private key:Used to generate HSP ECDH public key:Used to generate
HSM HMAC key		HSM GSRAM:Plaintext	Until the module is reset	Power-on reset	
HSM key derivation key		HSM GSRAM:Plaintext	Until the module is reset	Power-on reset	HSM AES Key:Used to generate HSM HMAC

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					key:Used to generate
Fuse secrets		Fuses:Plaintext	Until fuse zeroization is performed	Fuse zeroization	HSP key derivation key:Used to derive
HSP key derivation key		HSP KSU:Plaintext	Until the module is reset	Power-on reset	Fuse secrets:Derived From HSP ECDSA private key (DICE):Used to derive
HSP ECDSA private key (DICE)		HSP KSU:Plaintext	Until the module is reset	Power-on reset	HSP key derivation key:Derived From

Table 22: SSP Table 2

9.5 Transitions

Beginning in 2031, keys providing 112 bits of security strength shall no longer be used to apply cryptographic protection and are limited to legacy use for processing, as specified in Table 4 of NIST SP 800-57 Part 1 Rev. 5.

10 Self-Tests

10.1 Pre-Operational Self-Tests

N/A for this module.

The module does not perform any pre-operational test.

The integrity test is not applied for ROM firmware as the vendor claims the memory technology will not degrade for 10 years after the date of manufacture, in compliance with FIPS 140-3 IG 5.A. The end-of-life procedures described in Section 11.4 of this Security Policy shall be followed before 10 years have elapsed from the date of manufacture.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HSP AES-GCM (encryption)	256-bit key	KAT	CAST	Implied by successful operation of the module	Encryption	Power-up
HSP AES-GCM (decryption)	256-bit key	KAT	CAST	Implied by successful operation of the module	Decryption	Power-up
RSA KeyGen	2048 bits	PCT	PCT	Implied by successful operation of the module	Encryption & decryption	After every RSA key generation
HSP KBKDF	HMAC-SHA2-384; 384-bit key	KAT	CAST	Implied by successful operation of the module	Key based key derivation function	Power-up
HSP HMAC_DRBG	512-bit entropy input for instantiation; 512-bit entropy input for reseeding	KAT	CAST	Implied by successful operation of the module	Deterministic Random Bit Generator; instantiate, generate and reseed health test per section 11.3 of the SP 800-90Ar1	Power-up
HSP HKDF	HMAC-SHA-256; 176-bit input key; 104-bit salt;	KAT	CAST	Implied by successful operation of the module	HMAC based key derivation function	Power-up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	592-bit output key					
HSP AES-KWP (wrapping)	256-bit key	KAT	CAST	Implied by successful operation of the module	Key wrapping	Power-up
HSP AES-KWP (unwrapping)	256-bit key	KAT	CAST	Implied by successful operation of the module	Key unwrapping	Power-up
HSP ECDH SSC	P-384	KAT	CAST	Implied by successful operation of the module	Shared secret computation	Power-up
HSP ECDH KeyGen	N/A	PCT	PCT	Implied by successful operation of the module	Re-calculation of public key	After every HSP ECDH key generation
HSP ECDSA SigVer (ROM)	P-384 with SHA-384	KAT	CAST	Implied by successful operation of the module	Signature verification	Before the integrity/load test is performed
HSM AES-ECB	256-bit	KAT	CAST	Implied by successful operation of the module	Decryption	Power-up
HSM AES-KWP	256-bit	KAT	CAST	Implied by successful operation of the module	Key unwrapping	Power-up
HSM KBKDF	HMAC-SHA-512; 512-bit input key; 320-bit output key	KAT	CAST	Implied by successful operation of the module	Key-based key derivation function	Power-up
HSM HKDF	HMAC-SHA-256; 256-bit input key; 256-bit output key	KAT	CAST	Implied by successful operation of the module	HMAC-based key derivation function	Power-up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HSM AES-CBC (encryption)	256-bit key	KAT	CAST	Implied by successful operation of the module	Encryption	Power-up
HSM AES-CBC (decryption)	256-bit key	KAT	CAST	Implied by successful operation of the module	Decryption	Power-up
HSM AES-XTS (encryption)	256-bit key	KAT	CAST	Implied by successful operation of the module	Encryption	Power-up
HSM AES-XTS (decryption)	256-bit key	KAT	CAST	Implied by successful operation of the module	Decryption	Power-up
HSM HMAC_DRBG	1024-bit entropy input for instantiation; 512-bit entropy input for reseeding	KAT	CAST	Implied by successful operation of the module	Deterministic Random Bit Generator	Power-up
16 Self-tests of the 16 HSM RSA-OAEP Un-encapsulation Implementations (one self-test on each of the 16 UPKA instances)	2048 bit modulus; SHA-256	KAT	CAST	Implied by successful operation of the module	Un-encapsulation	Power-up
16 Self-tests of the 16 HSM RSA Signature Generation Component (with internal RSA acceleration) Implementations (one self-test on each of the 16 UPKA instances)	2048 bit modulus	KAT	CAST	Implied by successful signature generation	Signature Generation	Power-up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
16 Self-tests of the 16 HSM ECDSA Signature Generation Component Implementations (one self-test on each of the 16 UPKA instances)	P-384	KAT	CAST	Implied by successful operation of the module	Signature generation component	Power-up
16 Self-tests of the 16 HSM ECDH Implementations (one self-test on each of the 16 UPKA instances)	P-384	KAT	CAST	Implied by successful operation of the module	Shared secret computation	Power-up
HSM ECDSA KeyGen	SHA-256 for P-256; SHA-384 for P-384; SHA-512 for P-512	PCT	PCT	Implied by successful operation of the module	Sign & verify	After every HSM ECDSA key generation operation
HSM ECDH KeyGen	N/A	PCT	PCT	Implied by successful operation of the module	Shared secret computation	After every HSM ECDH key generation operation
Start-up APT for HSM entropy source	APT cutoff: 802; 1024 samples	APT	CAST	Implied by successful operation of the module	SP 800-90B health tests	Power-up
Start-up RCT for HSM entropy source	RCT cutoff: 51; 1024 samples	RCT	CAST	Implied by successful operation of the module	SP 800-90B health tests	Power-up
Continuous APT for HSM entropy source	APT cutoff: 802; 1024 samples	APT	CAST	Implied by successful operation of the module	SP 800-90B health tests	Power-up
Continuous RCT for HSM entropy source	RCT cutoff: 51	RCT	CAST	Implied by successful operation of the module	SP 800-90B health tests	Power-up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Start-up APT for HSP entropy source	APT cutoff: 802; 1024 samples	APT	CAST	Implied by successful operation of the module	SP 800-90B health tests	Power-up
Start-up RCT for HSP entropy source	RCT cutoff: 51; 1024 samples	RCT	CAST	Implied by successful operation of the module	SP 800-90B health tests	Power-up
Continuous APT for HSP entropy source	APT cutoff: 802; 1024 samples	APT	CAST	Implied by successful operation of the module	SP 800-90B health tests	Power-up
Continuous RCT for HSP entropy source	RCT cutoff: 51	RCT	CAST	Implied by successful operation of the module	SP 800-90B health tests	Power-up
HSP SHA-512	N/A	KAT	CAST	Implied by successful operation of the module	Hash function	Power-up
HSP ECDSA SigVer (run-time implementation)	P-384 with SHA-384	KAT	CAST	Implied by successful operation of the module	Signature verification	Power-up
HSP ECDSA SigGen for DICE attestation (run-time implementation)	P-384 with SHA-384	KAT	CAST	Implied by successful operation of the module	Signature generation	Power-up
HSP ECDSA SigVer Load Test (executed by ROM FW)	P-384 with SHA-384	FW load test	SW/FW Load	Implied by successful operation of the module; implied by successful completion of the firmware update service	Signature verification	On power-up; when the firmware update service is requested

Table 23: Conditional Self-Tests

10.3 Periodic Self-Test Information

N/A for this module.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HSP AES-GCM (encryption)	KAT	CAST	Once every 15 seconds	Automatically by the module without external input or control
HSP AES-GCM (decryption)	KAT	CAST	Once every 15 seconds	Automatically by the module without external input or control
RSA KeyGen	PCT	PCT	N/A	N/A
HSP KBKDF	KAT	CAST	Once every 15 seconds	Automatically by the module without external input or control
HSP HMAC_DRBG	KAT	CAST	Once every 15 seconds	Automatically by the module without external input or control
HSP HKDF	KAT	CAST	Once every 15 seconds	Automatically by the module without external input or control
HSP AES-KWP (wrapping)	KAT	CAST	Once every 15 seconds	Automatically by the module without external input or control
HSP AES-KWP (unwrapping)	KAT	CAST	Once every 15 seconds	Automatically by the module without external input or control
HSP ECDH SSC	KAT	CAST	Once every 15 seconds	Automatically by the module without external input or control
HSP ECDH KeyGen	PCT	PCT	N/A	N/A
HSP ECDSA SigVer (ROM)	KAT	CAST	Once every 15 seconds	Automatically by the module

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				without external input or control
HSM AES-ECB	KAT	CAST	Once every 60 seconds	Automatically by the module without external input or control
HSM AES-KWP	KAT	CAST	Once every 60 seconds	Automatically by the module without external input or control
HSM KBKDF	KAT	CAST	Once every 60 seconds	Automatically by the module without external input or control
HSM HKDF	KAT	CAST	Once every 60 seconds	Automatically by the module without external input or control
HSM AES-CBC (encryption)	KAT	CAST	Once every 60 seconds	Automatically by the module without external input or control
HSM AES-CBC (decryption)	KAT	CAST	Once every 60 seconds	Automatically by the module without external input or control
HSM AES-XTS (encryption)	KAT	CAST	Once every 60 seconds	Automatically by the module without external input or control
HSM AES-XTS (decryption)	KAT	CAST	Once every 60 seconds	Automatically by the module without external input or control
HSM HMAC_DRBG	KAT	CAST	Once every 60 seconds	Automatically by the module without external input or control
16 Self-tests of the 16 HSM RSA-OAEP Un-encapsulation	KAT	CAST	Once every 60 seconds	Automatically by the module without external input or control

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Implementations (one self-test on each of the 16 UPKA instances)				
16 Self-tests of the 16 HSM RSA Signature Generation Component (with internal RSA acceleration) Implementations (one self-test on each of the 16 UPKA instances)	KAT	CAST	Once every 60 seconds	Automatically by the module without external input or control
16 Self-tests of the 16 HSM ECDSA Signature Generation Component Implementations (one self-test on each of the 16 UPKA instances)	KAT	CAST	Once every 60 seconds	Automatically by the module without external input or control
16 Self-tests of the 16 HSM ECDH Implementations (one self-test on each of the 16 UPKA instances)	KAT	CAST	Once every 60 seconds	Automatically by the module without external input or control
HSM ECDSA KeyGen	PCT	PCT	N/A	N/A
HSM ECDH KeyGen	PCT	PCT	N/A	N/A
Start-up APT for HSM entropy source	APT	CAST	On-demand	By requesting the self-test service
Start-up RCT for HSM entropy source	RCT	CAST	On-demand	By requesting the self-test service
Continuous APT for HSM entropy source	APT	CAST	Continuously	Continuously as the noise source generates data

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Continuous RCT for HSM entropy source	RCT	CAST	Continuously	Continuously as the noise source generates data
Start-up APT for HSP entropy source	APT	CAST	On-demand	By requesting the self-test service
Start-up RCT for HSP entropy source	RCT	CAST	On-demand	By requesting the self-test service
Continuous APT for HSP entropy source	APT	CAST	Continuously	Continuously as the noise source generates data
Continuous RCT for HSP entropy source	RCT	CAST	Continuously	Continuously as the noise source generates data
HSP SHA-512	KAT	CAST	Once every 15 seconds	Automatically by the module without external input or control
HSP ECDSA SigVer (run-time implementation)	KAT	CAST	Once every 15 seconds	Automatically by the module without external input or control
HSP ECDSA SigGen for DICE attestation (run-time implementation)	KAT	CAST	Once every 15 seconds	Automatically by the module without external input or control
HSP ECDSA SigVer Load Test (executed by ROM FW)	FW load test	SW/FW Load	N/A	N/A

Table 24: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Normal Crash	The module crashes.	Failure of any self-test except for the start-up HSP APT/RCT,	The module automatically detects that it	Implicit indicator: for around 1 second, the module becomes unresponsive to any input and all data output and cryptographic operations

Name	Description	Conditions	Recovery Method	Indicator
		and continuous HSM APT/RCT	crashed and resets itself.	are blocked; after around 1 second, the module automatically recovers from the error state by resetting itself (which triggers the pre-operational self-tests and power-on CASTs)
Hard Crash	The module crashes and must be power cycled to recover from this hard crash.	Failure of the start-up HSP APT/RCT or continuous HSM APT/RCT	Power cycle of the module	Implicit indicator: the module becomes unresponsive to any input and all data output and cryptographic operations are blocked; the module does not automatically recover from the error state - the operator must power cycle the module to clear the error state.

Table 25: Error States

All data output through the data output interface and all cryptographic operations are inhibited in every error state.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module does not require any user installation or configuration after delivery from the silicon manufacturing facility.

11.2 Administrator Guidance

The module must be inspected physically for tamper evidence before use.

The operator must invoke the module name service and verify that it returns “Microsoft HSM Cryptographic Module”.

The operator must invoke the module version service and verify that it returns “3.4.2.3-50917001fips” for the boot-time firmware, “3.3.6.4-60108004fips” for the run-time firmware, and “M1244265-004 B0” for the HW and ROM FW version.

11.3 Non-Administrator Guidance

There is no non-administrator guidance.

11.4 End of Life

When the module needs to be securely sanitized, the operator must perform the zeroization method “Power-on reset” and then perform the zeroization method “Fuse zeroization” as described in Section 9.3 of this Security Policy.

When the module needs to be securely destroyed, it must be transitioned to the RETEST state.

12 Mitigation of Other Attacks

This module does not implement security mechanisms to mitigate other attacks. Therefore, this section is not applicable.

A Glossary and Abbreviations

AES	Advanced Encryption Standard
API	Application Programming Interface
CAST	Cryptographic Algorithm Self-Test
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
EFP/EFT	Environmental Failure Protection/Environmental Failure Testing
ESV	Entropy Source Validation
FIPS	Federal Information Processing Standard
GCM	Galois Counter Mode
HMAC	Keyed-Hash Message Authentication Code
IG	Implementation Guidance
IV	Initialization Vector
KAT	Known Answer Test
KSU	Key Storage Unit
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
PCT	Pair-wise Consistency Test
PSP	Public Security Parameter
ROM	Read Only Memory
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SSP	Sensitive Security Parameter
XTS	XEX-based Tweaked-codebook mode with Cipher Text Stealing