



Nuvoton Technology Corporation

## Nuvoton NPCT7xx TPM 2.0 Cryptographic Engine

Hardware Version 0x00FC

Firmware Version 7.2.5.1

### FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.2

Last update: 2026-02-13

Prepared by:

atsec information security corporation

4516 Seton Center Parkway, Suite 250

Austin, TX 78759

[www.atsec.com](http://www.atsec.com)

© 2025 Nuvoton / atsec information security.

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

# Table of Contents

- 1 General .....5
  - 1.1 Overview.....5
  - 1.2 Security Levels .....5
- 2 Cryptographic Module Specification .....6
  - 2.1 Description.....6
  - 2.2 Tested and Vendor Affirmed Module Version and Identification .....6
  - 2.3 Excluded Components.....7
  - 2.4 Modes of Operation .....7
  - 2.5 Algorithms.....8
  - 2.6 Security Function Implementations .....11
  - 2.7 Algorithm Specific Information .....15
  - 2.8 RBG and Entropy.....15
  - 2.9 Key Generation.....16
  - 2.10 Key Establishment .....16
  - 2.11 Industry Protocols .....16
- 3 Cryptographic Module Interfaces .....17
  - 3.1 Ports and Interfaces.....17
- 4 Roles, Services, and Authentication.....18
  - 4.1 Authentication Methods .....18
  - 4.2 Roles .....18
  - 4.3 Approved Services.....18
  - 4.4 Non-Approved Services .....66
  - 4.5 External Software/Firmware Loaded.....68
- 5 Software/Firmware Security .....69
  - 5.1 Integrity Techniques .....69
  - 5.2 Initiate on Demand.....69
- 6 Operational Environment .....70
  - 6.1 Operational Environment Type and Requirements .....70
- 7 Physical Security.....71
  - 7.1 Mechanisms and Actions Required .....71
  - 7.2 EFP/EFT Information.....71
  - 7.3 Hardness Testing Temperature Ranges .....71
- 8 Non-Invasive Security .....72
- 9 Sensitive Security Parameters Management .....73
  - 9.1 Storage Areas.....73
  - 9.2 SSP Input-Output Methods.....73
  - 9.3 SSP Zeroization Methods .....76

9.4 SSPs.....77

9.5 Transitions ..... 108

10 Self-Tests ..... 109

10.1 Pre-Operational Self-Tests ..... 109

10.2 Conditional Self-Tests..... 109

10.3 Periodic Self-Test Information..... 113

10.4 Error States..... 114

10.5 Operator Initiation of Self-Tests ..... 115

11 Life-Cycle Assurance ..... 116

11.1 Installation, Initialization, and Startup Procedures ..... 116

11.2 Administrator Guidance ..... 116

11.3 Non-Administrator Guidance..... 116

12 Mitigation of Other Attacks ..... 117

References..... 118

## 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 .....	10
Table 5: Vendor-Affirmed Algorithms .....	10
Table 6: Non-Approved, Not Allowed Algorithms .....	10
Table 7: Security Function Implementations .....	15
Table 8: Entropy Certificates .....	15
Table 9: Entropy Sources .....	15
Table 10: Ports and Interfaces .....	17
Table 11: Roles .....	18
Table 12: Approved Services .....	66
Table 13: Non-Approved Services .....	68
Table 14: Mechanisms and Actions Required .....	71
Table 15: EFP/EFT Information .....	71
Table 16: Hardness Testing Temperatures .....	71
Table 17: Storage Areas .....	73
Table 18: SSP Input-Output Methods .....	75
Table 19: SSP Zeroization Methods .....	77
Table 20: SSP Table 1 .....	88
Table 21: SSP Table 2 .....	108
Table 22: Pre-Operational Self-Tests .....	109
Table 23: Conditional Self-Tests .....	112
Table 24: Pre-Operational Periodic Information .....	113
Table 25: Conditional Periodic Information .....	114
Table 26: Error States .....	115

## List of Figures

Figure 1: Block Diagram .....	6
Figure 2: Hardware Module Photographs .....	7

# 1 General

## 1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the Nuvoton NPCT7xx TPM 2.0 Cryptographic Engine (hereafter referred to as “the module”). It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS 140-3 (Federal Information Processing Standards Publication 140-3). This Security Policy is Non-Proprietary and may be reproduced and distributed, but only whole and intact and including this notice.

## 1.2 Security Levels

The module meets the requirements of FIPS Pub 140-3 overall Security Level 1 with Physical Security section meeting Security Level 3.

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

Table 1: Security Levels

## 2 Cryptographic Module Specification

### 2.1 Description

**Purpose and Use:**

The Nuvoton NPCT7xx TPM 2.0 Cryptographic Engine is a hardware cryptographic module (hereafter simply referred to as “the module”) that implements advanced cryptographic algorithms, including symmetric and asymmetric cryptography, as well as key generation and random number generation. The module is a contained within a single-chip embodiment that provides cryptographic services utilized by external applications. The module meets commercial-grade specifications for power, temperature, reliability, shock, and vibrations, and includes chip packaging to meet the physical security requirements at security level 3.

**Module Type:** Hardware

**Module Embodiment:** SingleChip

**Cryptographic Boundary:**

The block diagram below shows the cryptographic boundary of the module, and its interfaces with the operational environment. The cryptographic boundary encompasses the entire physical chip. The single-chip is encased in three different package types that are identical except the physical dimensions and pin layouts.

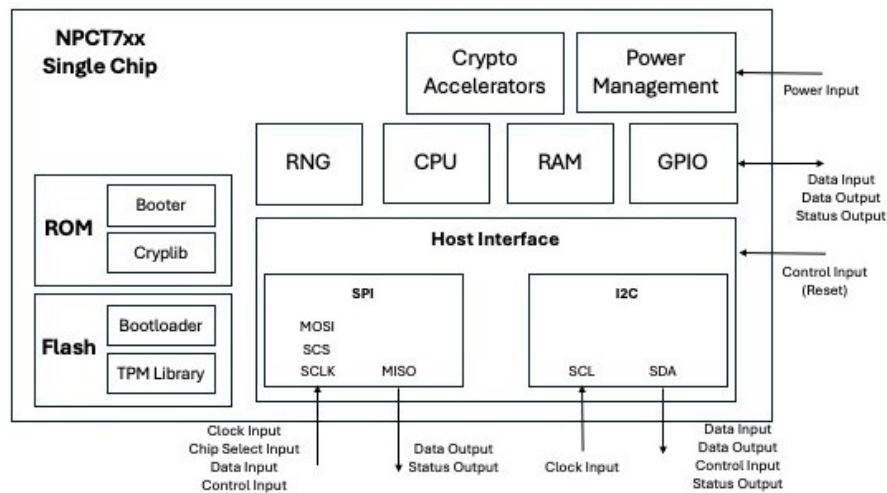


Figure 1: Block Diagram

### 2.2 Tested and Vendor Affirmed Module Version and Identification

**Tested Module Identification – Hardware:**

This module is available in three hardware configurations.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
NPCT7xx embedded in UQFN16 package	0x00FC	7.2.5.1	NPCT7xx CPU	N/A
NPCT7xx embedded in QFN32 package	0x00FC	7.2.5.1	NPCT7xx CPU	N/A

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
NPCT7xx embedded in TSSOP28 package	0x00FC	7.2.5.1	NPCT7xx CPU	N/A

Table 2: Tested Module Identification – Hardware

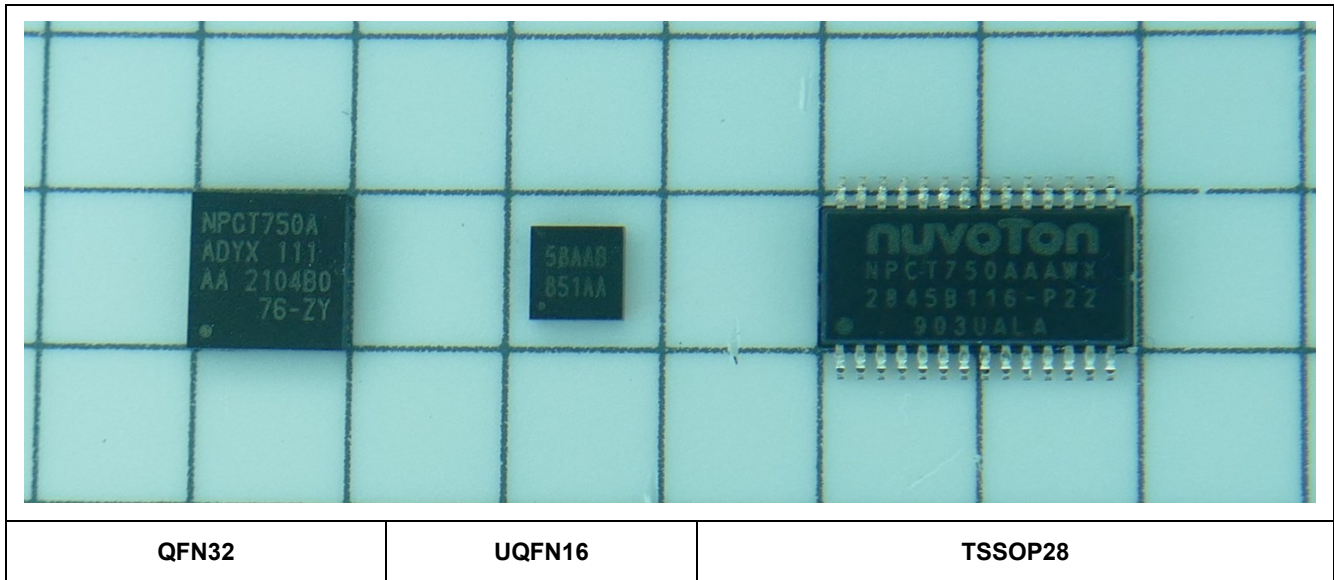


Figure 2: Hardware Module Photographs

### 2.3 Excluded Components

There are no components within the cryptographic boundary excluded from the FIPS 140-3 requirements.

### 2.4 Modes of Operation

#### Modes List and Description:

For some TPM host platforms, it might take too much time to execute all self-tests during power up. Therefore, the TPM supports the following two Approved modes.

Mode Name	Description	Type	Status Indicator
Transient mode	Default mode entered when the TPM powers up and has completed self tests for SHA-1, SHA2-256, SHA2-384, HMAC, AES, DRBG, KDF algorithms which are used for basic TPM commands.	Approved	Non-security relevant services are set to '00', approved services are set to '01'
Full approved mode of operation	This mode can be entered explicitly by calling TPM2_SelfTest command which will force the module to execute all conditional cryptographic algorithm self-tests at once. The mode is also entered implicitly when any TPM2 command is called which utilizes algorithms not tested in transient mode.	Approved	Non-security relevant services are set to '00', approved services are set to '01'
Non-Approved	Automatically entered whenever a non-approved service is invoked.	Non-Approved	'10'

Mode Name	Description	Type	Status Indicator
mode of operation			

Table 3: Modes List and Description

## 2.5 Algorithms

### Approved Algorithms:

The table below lists all approved algorithms used by the module, including specific key strengths employed for approved services, and implemented modes of operation.

Algorithm	CAVP Cert	Properties	Reference
AES-CFB128	A6386	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CTR	A6386	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-GCM	A6386	Direction - Decrypt, Encrypt IV Generation - External Key Length - 256	SP 800-38D
AES-OFB	A6386	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
Counter DRBG	A6386	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - No	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A6386	Curve - P-256, P-384 Secret Generation Mode - extra bits	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6386	Curve - P-256, P-384	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6386	Curve - P-256, P-384 Hash Algorithm - SHA2-256, SHA2-384 Component - No, Yes	FIPS 186-5
ECDSA SigVer (FIPS186-4)	A6386	Curve - P-256, P-384 Hash Algorithm - SHA-1	FIPS 186-4
ECDSA SigVer (FIPS186-5)	A6386	Curve - P-256, P-384 Hash Algorithm - SHA2-256, SHA2-384	FIPS 186-5
HMAC-SHA-1	A6386	Key Length - Key Length: 160-240 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6386	Key Length - Key Length: 160-1024 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6386	Key Length - Key Length: 160-2048 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
KAS-ECC Sp800-56Ar3	A6386	Domain Parameter Generation Methods - P-256, P-384 Function - Key Pair Generation, Partial Validation Scheme - fullUnified - KAS Role - Initiator, Responder KDF Methods - oneStepKdf - Key Length - 1024	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A6386	Domain Parameter Generation Methods - P-256, P-384 Scheme - fullUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDA HKDF Sp800-56Cr1	A6386	Derived Key Length - 384 Shared Secret Length - Shared Secret Length: 384 HMAC Algorithm - SHA2-384	SP 800-56C Rev. 2
KDA OneStep Sp800-56Cr1	A6386	Derived Key Length - 1024 Shared Secret Length - Shared Secret Length: 384-768 Increment 8	SP 800-56C Rev. 2
KDF SP800-108	A6386	KDF Mode - Counter Supported Lengths - Supported Lengths: 20, 48	SP 800-108 Rev. 1
KTS-IFC	A6386	Modulo - 2048, 3072, 4096 Key Generation Methods - rsakpg1-crt Scheme - KTS-OAEP-basic - KAS Role - initiator, responder Key Transport Method - Key Length - 384	SP 800-56B Rev. 2
RSA KeyGen (FIPS186-5)	A6386	Key Generation Mode - probable Modulo - 2048, 3072, 4096 Primality Tests - 2powSecStr Private Key Format - crt	FIPS 186-5
RSA SigGen (FIPS186-5)	A6386	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA Signature Primitive (CVL)	A6386	Private Key Format - crt	FIPS 186-4
RSA SigVer (FIPS186-4)	A6386	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-5)	A6386	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
SHA-1	A6386	Message Length - Message Length: 0-16384 Increment 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-256	A6386	Message Length - Message Length: 0-16384 Increment 8	FIPS 180-4
SHA2-384	A6386	Message Length - Message Length: 0-16384 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

**Vendor-Affirmed Algorithms:**

The following table lists all vendor affirmed approved algorithms implemented by the module.

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric and Asymmetric	N/A	SP 800-133 Rev2 Section 4 example 1

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:**

The following table list all non-approved algorithms not allowed in the approved mode of operation.

Name	Use and Function
RSA signature generation using SHA-1	Digital signature generation
ECDSA signature generation using SHA-1	Digital signature generation
ECDSA signature verification component	Digital signature verification of a message digest
RSA Key Transport	RSA Key Transport with Non-Approved Padding schemes RSAES-PKCS-v1.5/NULL
CKG	HMAC key generation with Key Size < 112 bits
HMAC	Message Authentication Code using HMAC with Key Size < 112 bits
KAS-ECC-SSC	ECC Shared Secret Computation with known seed

Table 6: Non-Approved, Not Allowed Algorithms

## 2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
AES-CFB128	BC-UnAuth	AES encryption/decryption	Key Size:128, 256 bits Key Strength:128, 256 bits	AES-CFB128: (A6386)
AES-CTR	BC-UnAuth	AES encryption/decryption	Key Size:128, 256 bits Key Strength:128, 256 bits	AES-CTR: (A6386)
AES-OFB	BC-UnAuth	AES encryption/decryption	Key Size:128, 256 bits Key Strength:128, 256 bits	AES-OFB: (A6386)
CTR_DRBG	DRBG	Deterministic random bit generation	Mode:AES-256 Key Size:256 bits Key Strength:256 bits Prediction Resistance:No Supports Reseed:Yes Derivation Function Enabled:No	Counter DRBG: (A6386)
ECDSA KeyGen	AsymKeyPair-KeyGen	ECC key generation	Curves:P-256, P-384 Key Strength:128 and 192 bits	ECDSA KeyGen (FIPS186-5): (A6386) CKG: ()
ECDSA KeyVer	AsymKeyPair-KeyVer	ECC public key validation	Curves:P-256, P-384 Key Strength:128 and 192 bits	ECDSA KeyVer (FIPS186-5): (A6386)
ECDSA SigGen	DigSig-SigGen	ECC signature generation	Curves:P-256, P-384 Key Strength:128 and 192 bits Hash Algorithm:SHA2-256, SHA2-384	ECDSA SigGen (FIPS186-5): (A6386)
ECDSA SigVer	DigSig-SigVer	ECC signature verification	Curves:P-256, P-384 Key Strength:128 and 192 bits Hash Algorithm:SHA2-256, SHA2-384	ECDSA SigVer (FIPS186-5): (A6386)
ECDSA SigVer (legacy)	DigSig-SigVer	ECC signature verification with SHA-1	Curves:P-256, P-384 Key Strength:128 and 192 bits Hash Algorithm:SHA-1	ECDSA SigVer (FIPS186-4): (A6386)

Name	Type	Description	Properties	Algorithms
ECDSA SigGen Component	DigSig-SigGen	ECC signature generation component	Curves:P-256, P-384 Key Strength:128 and 192 bits	ECDSA SigGen (FIPS186-5): (A6386)
HMAC	MAC	Message Authentication Code using HMAC	Key sizes:160, 256, 384 bits Key Strength:160, 256, 384 bits	HMAC-SHA-1: (A6386) HMAC-SHA2-256: (A6386) HMAC-SHA2-384: (A6386)
KAS-ECC	KAS-Full	ECC key agreement	IG:IG D.F scenario 2, path (2) Key confirmation:no Key derivation:KDA (tested as part KAS certificate) Caveat:Key establishment methodology provides between 128 and 192 bits of security strength	KAS-ECC Sp800-56Ar3: (A6386)
KAS-ECC-SSC	KAS-SSC	ECC shared secret computation	Key Agreement Schemes:Full Unified, One Pass DH Curves:P-256, P-384 Key Strength:128 and 192 bits	KAS-ECC-SSC Sp800-56Ar3: (A6386)
KDA	KAS-56CKDF	Symmetric key derivation	Auxiliary Function Methods:SHA2-256, SHA2-384 Key Size:160, 256, 384 bits Key Strength:160, 256, 384 bits	KDA OneStep Sp800-56Cr1: (A6386)
KBKDF	KBKDF	Symmetric key derivation	KDF Mode:Counter Mac Mode:HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384 Key Size:160, 256, 384 bits Key Strength:160, 256, 384 bits	KDF SP800-108: (A6386)
KTS RSA	KTS-Decap KTS-Encap	RSA key transport	Standard:SP 800-56Brev2 IG D.G:Approved RSA-based key transport scheme Key confirmation:no Caveat:Key	KTS-IFC: (A6386)

Name	Type	Description	Properties	Algorithms
			encapsulation methodology providing between 112 to 150 bits of key strength Scheme:KTS-OAEP-basic Modulus Size:2048, 3072, 4096	
RSA KeyGen	AsymKeyPair-KeyGen	RSA key generation	Key Generation Mode:B.3.3 Key Size:2048, 3072, 4096 bits Key Strength:112, 128, 150 bits	RSA KeyGen (FIPS186-5): (A6386) CKG: ()
RSA SigGen	DigSig-SigGen	RSA signature generation	Signature Type:PKCS 1.5, PKCSPSS Hash Pair:SHA2-256, SHA2-384 Key Size:2048, 3072, 4096 bits Key Strength:112, 128, 150 bits	RSA SigGen (FIPS186-5): (A6386)
RSA SigGen Primitive	DigSig-SigGen	RSA signature generation primitive	Key Size:2048, 3072, 4096 bits Key Strength:112, 128, 150 bits	RSA Signature Primitive: (A6386)
RSA SigVer	DigSig-SigVer	RSA signature verification	Signature Type:PKCS 1.5, PKCSPSS Hash Pair:SHA2-256, SHA2-384 Key Size:2048, 3072, 4096 bits Key Strength:112, 128, 150 bits	RSA SigVer (FIPS186-5): (A6386)
RSA SigVer (legacy)	DigSig-SigVer	RSA signature verification with SHA-1	Signature Type:PKCS 1.5, PKCSPSS Hash Pair:SHA-1 Key Size:2048, 3072, 4096 bits Key Strength:112, 128, 150 bits	RSA SigVer (FIPS186-4): (A6386)
SHA	SHA	Message digest		SHA-1: (A6386) SHA2-256: (A6386) SHA2-384: (A6386)
AES key generation	CKG	AES key generation	Key Size:128, 256 bits Key Strength:128, 256 bits	Counter DRBG: (A6386) CKG: ()

Name	Type	Description	Properties	Algorithms
HMAC key generation	CKG	HMAC key generation	Key Size:160, 256, 384 bits Key Strength:160, 256, 384 bits	Counter DRBG: (A6386) CKG: ()
KTS (AES + HMAC) key wrapping	KTS-Wrap	SP 800-38F key wrapping, per IG D.G	Standard:SP 800-38F IG D.G:Approved symmetric key-wrapping technique using AES-CFB128 and HMAC Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-CFB128: (A6386) HMAC-SHA-1: (A6386) HMAC-SHA2-256: (A6386) HMAC-SHA2-384: (A6386)
KTS (AES + HMAC) key unwrapping	KTS-Unwrap	SP 800-38F key unwrapping, per IG D.G	Standard:SP 800-38F IG D.G:Approved symmetric key-wrapping technique using AES-CFB128 and HMAC Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-CFB128: (A6386) HMAC-SHA-1: (A6386) HMAC-SHA2-256: (A6386) HMAC-SHA2-384: (A6386)
Entropy Source	ENT-ESV	Physical entropy source	Conditioning Component:Block Cipher DF using AES-256 Sample Size:1024 bits Entropy Per Sample:512 bits	Conditioning Component Block Cipher Derivation Function SP800-90B: (A6386)
HKDF	KAS-56CKDF	Symmetric key derivation (KDA)	HMAC Algorithm:HMAC-SHA2-384 Derived Key Length:384 bits Shared Secret Length:384 bits	KDA HKDF Sp800-56Cr1: (A6386)
AES-GCM	BC-Auth	AES authenticated encryption/decryption	Key Size:128, 192, 256 bits Key Strength:128, 192, 256 bits	AES-GCM: (A6386)
KAS-ECC-SSC + HKDF	KAS-Full	KAS-ECC-SSC + HKDF for SPDm protocol	IG:IG D.F scenario 2, path (2) Key confirmation:no	KAS-ECC-SSC Sp800-56Ar3: (A6386)

Name	Type	Description	Properties	Algorithms
			Key derivation:KDA (separately tested) Caveat:Key establishment methodology provides between 128 and 192 bits of security strength	KDA HKDF Sp800-56Cr1: (A6386)

Table 7: Security Function Implementations

## 2.7 Algorithm Specific Information

Compliance to IG C.K is met by obtaining CAVP certs according to FIPS 186-5.

The module generates GCM IV in compliance with scenario 5 of IG C.H. The IV length is 96 bits (32-bits 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 is used solely by the SPDM protocol.

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

FIPS 186-4 CAVP entries for RSA SigVer and ECDSA SigVer are present to provide legacy support for digital signature verification with SHA-1 with accordance to IG C.K additional comment 2. Algorithms designated as "Legacy" can only be used on data that was generated prior to the Legacy Date specified in FIPS 140-3 IG C.M.

## 2.8 RBG and Entropy

Cert Number	Vendor Name
E18	Nuvoton

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Nuvoton NPCT7xx TPM 2.0 Cryptographic Engine	Physical	Nuvoton NPCT7xx TPM 2.0 Cryptographic Engine on Nuvoton NPCT7xx	384 bits	Full entropy	Vetted Conditioning Component: Block Cipher Derivation Function using AES-256. Cert# A6386

Table 9: Entropy Sources

**RNG Information:** The module implements an approved SP 800-90Ar1 Deterministic Random Bit Generator in the form of CTR\_DRBG. The DRBG seed is generated from the SP 800-90B compliant entropy source.

## 2.9 Key Generation

This module implements symmetric and asymmetric key generation services for AES, HMAC, RSA, ECDSA and EC Diffie-Hellman keys, compliant to SP800-133rev2 Cryptographic Key Generation (CKG, vendor affirmed). When generating RSA and ECDSA keys, the seed (i.e., random value) used for asymmetric key generation is obtained directly from the module's approved SP800-90rev1 DRBG (CTR\_DRBG). This is followed by an asymmetric key generation method compliant with FIPS186-5 and defined in Section 4 example 1 of SP800-133rev2. The EC Diffie-Hellman keys are generated internally by the module using ECDSA key generation method compliant with FIPS186-5 and SP800-56Arev3 as defined in section 5.2 of SP800-133rev2.

Symmetric AES and HMAC keys are generated as defined in Section 4 example 1 of SP800-133rev2.

The module provides key derivation services using SP800-108 KBKDF, SP800-56Cr1 OneStep KDF and SP800-56Cr1 HKDF.

## 2.10 Key Establishment

The module provides an approved [SP800-56Arev3] EC Diffie-Hellman Key Agreement Scheme. The key agreement scheme is compliant with IG D.F scenario 2 path (2). The CAVP testing was performed end-to-end, using the Full Unified and One Pass DH Models with approved domain parameters (i.e., P-256 and P-384). A key derivation function is applied after shared secret computation as part of the Key Agreement Scheme.

Both encapsulation and un-encapsulation are supported for SP800-56Brev2 Key Transport using KTS-OAEP-basic.

### **Compliance to SP 800-56Arev3 assurances**

For KAS-ECC, the module satisfies IG D.F Scenario 2 path (2) (i.e., tested compliance with Full Unified and One Pass DH key agreement schemes followed by the derivation of the key as shown in Section 5.8 of SP 800-56Arev3). The key derivation function complies to SP 800-56C rev2 (i.e., One-Step KDF). Furthermore, the module obtained the appropriate assurances, as required in Sections 5.6.2 of SP 800-56A rev3.

### **Compliance to SP 800-56Brev2 assurances**

For KTS RSA, the implementation satisfies IG D.G by employing an approved RSA-based key transport scheme as specified in SP 800-56Brev2 and is tested with RSA 2048, 3072, 4096 modulus size keys. Both encapsulation and un-encapsulation are supported. The module obtained the appropriate assurances, as defined in Sections 5 and 6 of SP 800-56Brev2.

## 2.11 Industry Protocols

The cryptographic module implements the Security Protocol and Data Model (SPDM) standard protocol to facilitate secure communication between hardware and firmware components. The security function implementations used by SPDM framework includes HKDF using SHA2-384, AES-GCM using 256-bit keys, KAS-ECC-SSC using curve P-384 and ECDSA SigGen/SigVer using curve P-384 with SHA2-384.

## 3 Cryptographic Module Interfaces

### 3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
SPI MOSI Pin	Data Input Control Input	Data/Control provided to the chip as part of the data processing commands
SPI MISO Pin	Data Output Status Output	Data/Control provided by the chip as part of the data processing commands
I2C SDA Pin	Data Input Data Output Status Output Control Input	Data/Control provided to/by the chip as part of the data processing commands
Power	Power	Power interface of the chip
Reset	Control Input	physical control input pin used to reset the cryptographic module
GPIO	Data Input Data Output Status Output	Data provided to/by the chip
SPI SCLK Pin	None	Serial Clock Input
SPI SCS Pin	None	SPI Chip Select
I2C SCL Pin	None	Serial Clock Input

Table 10: Ports and Interfaces

The logical interfaces are the TPM2 commands through which users of the module request services. The ports and interfaces are shown in the table above.

All data output via data output interface is inhibited when the module is performing pre-operational test or zeroization or when the module enters error state.

## 4 Roles, Services, and Authentication

### 4.1 Authentication Methods

N/A for this module.

The module does not support role authentication.

### 4.2 Roles

Name	Type	Operator Type	Authentication Methods
Object Administrator	Role	Crypto Officer	None
Object User	Role	User	None
Duplicate	Role	Crypto Officer	None

Table 11: Roles

### 4.3 Approved Services

The table below lists the approved services. For each service, the table lists the associated cryptographic algorithm(s), the role to perform the service, the cryptographic keys or SSPs involved, and their access type(s). The following convention is used to specify access rights for SSPs:

**G = Generate:** The module generates or derives the SSP.

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

**W = Write:** The SSP is updated, imported, or written to the module.

**E = Execute:** The module uses the SSP in performing a cryptographic operation.

**Z = Zeroize:** The module zeroizes the SSP.

**N/A:** The calling application does not access any SSP or key during its operation.

Details on the approved cryptographic algorithms, can be found in the SFI table. The module implements a FIPS 140-3 service indicator query function that outputs its value. This value corresponds to the three categories defined in IG 2.4.C. **Non-security relevant** services are set to '00', **approved services** are set to '01' and **non-approved services** are set to '10'.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
TPM2_Startup	Used to initiate a startup process, where the TPM state is either reset or loaded from a saved state.	'00'	Startup Type	N/A	Entropy Source	Unauthenticated - nullSeed: Z - nullProof: Z - platformAuth: Z - platformPolicy: Z - endorsementP

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						olicity: Z - ownerPolicy: Z - lockoutPolicy: Z - Asymmetric Signing Keys (authValue): Z - Asymmetric Signing Keys (seedValue): Z - Asymmetric Signing Keys (sensitive data): Z - Asymmetric Signing Keys (authPolicy): Z - Asymmetric Signing Keys (public data): Z - Asymmetric Encryption Keys (authValue): Z - Asymmetric Encryption Keys (seedValue): Z - Asymmetric Encryption Keys (sensitive data): Z - Asymmetric Encryption Keys (authPolicy): Z - Asymmetric Encryption Keys (public data): Z - Symmetric Encryption Keys (authValue): Z - Symmetric Encryption Keys (seedValue): Z - Symmetric Encryption Keys

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(sensitive data): Z - Symmetric Signing Keys (authValue): Z - Symmetric Signing Keys (seedValue): Z - Symmetric Signing Keys (sensitive data): Z - Session (sessionKey): Z - DRBG state: Z - DRBG Entropy Input: G,Z - Transient DRBG state: Z
TPM2_Shutdown	Used to prepare the TPM for a power cycle.	'00'	Shutdown Type	N/A	None	Unauthenticated - nullSeed: Z - nullProof: Z - platformAuth: Z - platformPolicy: Z - endorsementPolicy: Z - ownerPolicy: Z - lockoutPolicy: Z - Asymmetric Signing Keys (authValue): Z - Asymmetric Signing Keys (seedValue): Z - Asymmetric Signing Keys (sensitive data): Z - Asymmetric Signing Keys (authPolicy): Z - Asymmetric Signing Keys

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(public data): Z - Asymmetric Encryption Keys (authValue): Z - Asymmetric Encryption Keys (seedValue): Z - Asymmetric Encryption Keys (sensitive data): Z - Asymmetric Encryption Keys (authPolicy): Z - Asymmetric Encryption Keys (public data): Z - Symmetric Encryption Keys (authValue): Z - Symmetric Encryption Keys (seedValue): Z - Symmetric Encryption Keys (sensitive data): Z - Symmetric Signing Keys (authValue): Z - Symmetric Signing Keys (seedValue): Z - Symmetric Signing Keys (sensitive data): Z - Session (sessionKey): Z - DRBG state: Z - DRBG Entropy Input: G,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Transient DRBG state: Z
TPM2_IncrementalSelfTest	Perform Self-Test of selected algorithms.	'01'	List of algorithms to be tested	To do list of the selected algorithms All algorithms mentioned in Table 22	AES-CFB128 AES-CTR AES-OFB CTR_DRBG ECDSA KeyGen ECDSA KeyVer ECDSA SigGen ECDSA SigVer HMAC KAS-ECC KAS-ECC-SSC KDA KBKDF KTS RSA RSA KeyGen RSA SigGen RSA SigGen Primitive RSA SigVer SHA HKDF AES-GCM	Unauthenticated
TPM2_SelfTest	Perform Self-Test of all functions or only those that have not previously been tested.	'01'	Choose whether to perform the test everything (fullTest = YES) or only the untested functions	N/A	AES-CFB128 AES-CTR AES-OFB CTR_DRBG ECDSA KeyGen ECDSA	Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			(fullTest = NO)		KeyVer ECDSA SigGen ECDSA SigVer HMAC KAS-ECC KAS-ECC-SSC KDA KBKDF KTS RSA RSA KeyGen RSA SigGen RSA SigGen Primitive RSA SigVer SHA HKDF AES-GCM	
TPM2_GetTestResult (Show Status)	Returns manufacturer-specific information regarding the results of a self-test and an indication of the test status.	'00'	N/A	test result data (manufacturer-specific information), test result	None	Unauthenticated
TPM2_StartAuthSession	Start authorization session.	'01'	asymmetric keys, session Type, encryption algorithm, key size, hash algorithm	session handle, TPM nonce	CTR_D RBG KAS-ECC KBKDF KTS RSA	Unauthenticated - platformAuth: E - Asymmetric Encryption Keys (authValue): E - Asymmetric Encryption Keys (seedValue): E - Asymmetric Encryption Keys (sensitive

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						data): E - Asymmetric Encryption Keys (authPolicy): E - Asymmetric Encryption Keys (public data): E - Ephemeral Key Agreement Keys: G,E - Session (salt): G,E - Session (sessionKey): G,E - Session (symKey): G,E - DRBG state: G - Transient DRBG state: G - DRBG Entropy Input: W
TPM2_PolicyRestart	Allows a policy authorization session to be returned to its initial state.	'00'	session handle	N/A	None	Unauthenticated Object User
TPM2_Create	Creation of an ordinary object.	'01'	Parent handle, sensitive data, public template, outside info, creationPCR	private portion, public portion, creation data, hash value, creation ticket (see TPM2_CertifyCreation)	CTR_D DRBG Entropy Source ECDSA KeyGen HMAC RSA KeyGen SHA KBKDF AES key generation HMAC key generation KTS	Object User - Asymmetric Signing Keys (authValue): G,R - Asymmetric Signing Keys (seedValue): G,R - Asymmetric Signing Keys (sensitive data): G,R - Asymmetric Signing Keys (authPolicy): G,R - Asymmetric Signing Keys (public data):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					(AES + HMAC) key unwrapping KTS (AES + HMAC) key wrapping	G,R - Asymmetric Encryption Keys (authValue): G,R - Asymmetric Encryption Keys (seedValue): G,R - Asymmetric Encryption Keys (sensitive data): G,R - Asymmetric Encryption Keys (authPolicy): G,R - Asymmetric Encryption Keys (public data): G,R - Symmetric Encryption Keys (authValue): G,R - Symmetric Encryption Keys (seedValue): G,R - Symmetric Encryption Keys (sensitive data): G,R - Symmetric Signing Keys (authValue): G,R - Symmetric Signing Keys (seedValue): G,R - Symmetric Signing Keys (sensitive data): G,R - DRBG state: G - Transient

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						DRBG state: G - DRBG Entropy Input: W
TPM2_Load	Loading an protected object.	'01'	Parent handle, private portion, public portion	Object handle, name of the loaded object	HMAC KAS-ECC-SSC KBKDF SHA KTS (AES + HMAC) key unwrap ping	Object User - Asymmetric Signing Keys (authValue): W - Asymmetric Signing Keys (seedValue): W - Asymmetric Signing Keys (sensitive data): W - Asymmetric Signing Keys (authPolicy): W - Asymmetric Signing Keys (public data): W - Asymmetric Encryption Keys (authValue): W - Asymmetric Encryption Keys (seedValue): W - Asymmetric Encryption Keys (sensitive data): W - Asymmetric Encryption Keys (authPolicy): W - Asymmetric Encryption Keys (public data): W - Symmetric Encryption Keys (authValue):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W - Symmetric Encryption Keys (seedValue): W - Symmetric Encryption Keys (sensitive data): W - Symmetric Signing Keys (authValue): W - Symmetric Signing Keys (seedValue): W - Symmetric Signing Keys (sensitive data): W - Object Ephemeral Keys (symKey): E - Object Ephemeral Keys (hmacKey): E - TPM ECDH Shared Secret: G
TPM2_LoadExternal	Loading an external object.	'01'	Private portion, public portion, associated hierarchy	Object handle, name of the loaded object	HMAC KAS- ECC- SSC SHA	Unauthenticated - Asymmetric Encryption Keys (authValue): W - Asymmetric Encryption Keys (seedValue): W - Asymmetric Encryption Keys (sensitive data): W - Asymmetric Encryption Keys

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(authPolicy): W - Asymmetric Encryption Keys (public data): W - Symmetric Encryption Keys (authValue): W - Symmetric Encryption Keys (seedValue): W - Symmetric Encryption Keys (sensitive data): W - Symmetric Signing Keys (authValue): W - Symmetric Signing Keys (seedValue): W - Symmetric Signing Keys (sensitive data): W - TPM ECDH Shared Secret: G
TPM2_ReadPublic	Allows access to the public area of a loaded object.	'00'	object handle	public area of object, name of object, qualified name of object	None	Unauthenticated - Asymmetric Signing Keys (authValue): R - Asymmetric Signing Keys (authPolicy): R - Asymmetric Signing Keys (public data): R - Asymmetric Encryption Keys (authValue): R - Asymmetric Encryption

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Keys (authPolicy): R - Asymmetric Encryption Keys (public data): R
TPM2_ActivateCredential	Decrypts an object credential.	'01'	active handle, key handle, credential blob, secret	decrypted certificate information	KAS- ECC KTS RSA	Object Administrator - Asymmetric Encryption Keys (authValue): E - Asymmetric Encryption Keys (seedValue): E - Asymmetric Encryption Keys (sensitive data): E - Asymmetric Encryption Keys (authPolicy): E - Asymmetric Encryption Keys (public data): E - Credential Ephemeral Keys (symKey): G - Credential Ephemeral Keys (hmacKey): G - Ephemeral Key Agreement Keys: E - TPM ECDH Shared Secret: G Object User - Asymmetric Encryption Keys (authValue): E - Asymmetric Encryption Keys (seedValue):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						E - Asymmetric Encryption Keys (sensitive data): E - Asymmetric Encryption Keys (authPolicy): E - Asymmetric Encryption Keys (public data): E - Credential Ephemeral Keys (symKey): G - Credential Ephemeral Keys (hmacKey): G - Ephemeral Key Agreement Keys: E - TPM ECDH Shared Secret: G
TPM2_MakeCredential	Encrypts object credential.	'01'	Object handle, credential, object name	encrypted secret, credentialBlob	CTR_D RBG KAS- ECC KTS RSA	Unauthenticated - Asymmetric Encryption Keys (authValue): E - Asymmetric Encryption Keys (seedValue): E - Symmetric Encryption Keys (sensitive data): E - Asymmetric Encryption Keys (authPolicy): E - Asymmetric Encryption Keys (public data): E - DRBG state:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G - Transient DRBG state: G - DRBG Entropy Input: W - Credential Ephemeral Keys (symKey): G,R - Credential Ephemeral Keys (hmacKey): G,R - Ephemeral Key Agreement Keys: E - TPM ECDH Shared Secret: G
TPM2_Unseal	Returns the data in a loaded Sealed Data Object.	'00'	item handle	unsealed data	None	Object User
TPM2_ObjectChangeAuth	Change the authorization secret of an object.	'01'	Object handle, parent handle, new authValue	private area containing new authValue	CTR_DRBG SHA KTS (AES + HMAC) key wrapping KTS (AES + HMAC) key unwrapping	Object Administrator - Asymmetric Signing Keys (authValue): R,W - Asymmetric Signing Keys (seedValue): R,W - Asymmetric Signing Keys (sensitive data): R,W - Asymmetric Signing Keys (authPolicy): R,W - Asymmetric Signing Keys (public data): R,W - Asymmetric Encryption Keys (authValue): R,W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						<ul style="list-style-type: none"> <li>- Asymmetric Encryption Keys (seedValue): R,W</li> <li>- Asymmetric Encryption Keys (sensitive data): R,W</li> <li>- Asymmetric Encryption Keys (authPolicy): R,W</li> <li>- Asymmetric Encryption Keys (public data): R,W</li> <li>- Symmetric Encryption Keys (authValue): R,W</li> <li>- Symmetric Encryption Keys (seedValue): R,W</li> <li>- Symmetric Encryption Keys (sensitive data): R,W</li> <li>- Symmetric Signing Keys (authValue): R,W</li> <li>- Symmetric Signing Keys (seedValue): R,W</li> <li>- Symmetric Signing Keys (sensitive data): R,W</li> <li>- Object Ephemeral Keys (symKey): G,R,E</li> <li>- Object Ephemeral Keys (hmacKey):</li> </ul>

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,R,E - DRBG state: G - Transient DRBG state: G - DRBG Entropy Input: W
TPM2_CreateLoaded	Creation and loading of an ordinary or a derived object.	'01'	Parent handle, private portion, public key portion	Object handle, private portion, public portion, Name of the loaded object	CTR_D RBG Entropy Source ECDSA KeyGen HMAC KDKDF RSA KeyGen SHA AES key generation HMAC key generation KTS (AES + HMAC) key wrapping	Object User - ppSeed: E - epSeed: E - spSeed: E - nullSeed: E - platformAuth: E - endorsementAuth: E - ownerAuth: E - Asymmetric Signing Keys (authValue): G,W - Asymmetric Signing Keys (seedValue): G,W - Asymmetric Signing Keys (sensitive data): G,W - Asymmetric Signing Keys (authPolicy): G,W - Asymmetric Signing Keys (public data): G,W - Asymmetric Encryption Keys (authValue): G,W - Asymmetric Encryption Keys (seedValue): G,W - Asymmetric Encryption Keys

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(sensitive data): G,W - Asymmetric Encryption Keys (authPolicy): G,W - Asymmetric Encryption Keys (public data): G,W - Symmetric Encryption Keys (authValue): G,W - Symmetric Encryption Keys (seedValue): G,W - Symmetric Encryption Keys (sensitive data): G,W - Symmetric Signing Keys (authValue): G,W - Symmetric Signing Keys (seedValue): G,W - Symmetric Signing Keys (sensitive data): G,W - Object Ephemeral Keys (symKey): G,W,E - Object Ephemeral Keys (hmacKey): G,W,E
TPM2_Duplicate	Duplicates a loaded object to a new parent object.	'01'	Object handle, new parent handle, encryption key,	Encrypted key, duplicate object, seed value	CTR_D RBG KAS- ECC KBKDF KTS	Duplicate - Asymmetric Encryption Keys (authValue): R,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			symmetric algorithm for key wrapping	(asymmetrically encrypted)	RSA SHA KTS (AES + HMAC) key wrapping	<ul style="list-style-type: none"> <li>- Asymmetric Encryption Keys (seedValue): R,E</li> <li>- Asymmetric Encryption Keys (sensitive data): R,E</li> <li>- Asymmetric Encryption Keys (authPolicy): R,E</li> <li>- Asymmetric Encryption Keys (public data): R,E</li> <li>- Duplication Ephemeral Keys (symKey): E</li> <li>- Duplication Ephemeral Keys (hmacKey): E</li> <li>- Ephemeral Key Agreement Keys: E</li> <li>- Asymmetric Signing Keys (authValue): R</li> <li>- Asymmetric Signing Keys (seedValue): R</li> <li>- Asymmetric Signing Keys (sensitive data): R</li> <li>- Asymmetric Signing Keys (authPolicy): R</li> <li>- Asymmetric Signing Keys (public data): R</li> <li>- Symmetric Encryption Keys (authValue): R</li> <li>- Symmetric Encryption</li> </ul>

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Keys (seedValue): R - Symmetric Encryption Keys (sensitive data): R - Symmetric Signing Keys (authValue): R - Symmetric Signing Keys (seedValue): R - Symmetric Signing Keys (sensitive data): R - DRBG state: G - Transient DRBG state: G - DRBG Entropy Input: W
TPM2_Rewrap	Rewraps a duplicated object with a new parent key.	'01'	Old parent, new parent, duplicate object, name of object to be wrapped, seed value for the symmetric key and HMAC key	New duplicate object, seed for new object (encrypted with new parent's asymmetric key)	CTR_D RBG KAS-ECC KBKDF KTS RSA KTS (AES + HMAC) key wrapping KTS (AES + HMAC) key unwrap ping	Object User - Duplication Ephemeral Keys (symKey): E - Duplication Ephemeral Keys (hmacKey): E - Ephemeral Key Agreement Keys: E - Asymmetric Signing Keys (authValue): R - Asymmetric Signing Keys (seedValue): R - Asymmetric Signing Keys (sensitive data): R - Asymmetric Signing Keys (authPolicy): R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						<ul style="list-style-type: none"> <li>- Asymmetric Signing Keys (public data): R</li> <li>- Asymmetric Encryption Keys (authValue): R</li> <li>- Asymmetric Encryption Keys (seedValue): R</li> <li>- Asymmetric Encryption Keys (sensitive data): R</li> <li>- Asymmetric Encryption Keys (authPolicy): R</li> <li>- Asymmetric Encryption Keys (public data): R</li> <li>- Symmetric Encryption Keys (authValue): R</li> <li>- Symmetric Encryption Keys (seedValue): R</li> <li>- Symmetric Encryption Keys (sensitive data): R</li> <li>- Symmetric Signing Keys (authValue): R</li> <li>- Symmetric Signing Keys (seedValue): R</li> <li>- Symmetric Signing Keys (sensitive data): R</li> <li>- DRBG state: G</li> <li>- Transient DRBG state:</li> </ul>

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G - DRBG Entropy Input: W
TPM2_Import	Import a duplicated object to be next loaded inside the TPM.	'01'	Parent handle, encryption key, public area of object to be imported, encrypted duplicate object, duplicate object seed, algorithm for key wrapping	Private portion encrypted with the symmetric key of parent handle	CTR_D RBG HMAC KAS- ECC KBDKF KTS RSA SHA KTS (AES + HMAC) key unwrap ping	Object User - Asymmetric Encryption Keys (authValue): R,E - Asymmetric Encryption Keys (seedValue): R,E - Asymmetric Encryption Keys (sensitive data): R,E - Asymmetric Encryption Keys (authPolicy): R,E - Asymmetric Encryption Keys (public data): R,E - Duplication Ephemeral Keys (symKey): E - Duplication Ephemeral Keys (innerSymKey): E - Ephemeral Key Agreement Keys: E - Asymmetric Signing Keys (authValue): R - Asymmetric Signing Keys (seedValue): R - Asymmetric Signing Keys (sensitive data): R - Asymmetric

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Signing Keys (authPolicy): R - Asymmetric Signing Keys (public data): R - Symmetric Encryption Keys (authValue): R - Symmetric Encryption Keys (seedValue): R - Symmetric Encryption Keys (sensitive data): R - Symmetric Signing Keys (authValue): R - Symmetric Signing Keys (seedValue): R - Symmetric Signing Keys (sensitive data): R - DRBG state: G - Transient DRBG state: G - DRBG Entropy Input: W
TPM2_RSA_Encrypt	RSA Encryption.	'01'	Key handle, message, padding scheme, label	Cipher text	KTS RSA	Unauthenticated - Asymmetric Encryption Keys (authValue): E - Asymmetric Encryption Keys (seedValue): E - Asymmetric Encryption Keys (sensitive

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						data): E - Asymmetric Encryption Keys (authPolicy): E
TPM2_RSA_Decrypt	RSA Decryption.	'01'	Key handle, cipher text, scheme, label	Plaintext	KTS RSA	Unauthenticated - Asymmetric Encryption Keys (authValue): E - Asymmetric Encryption Keys (seedValue): E - Asymmetric Encryption Keys (authPolicy): E - Asymmetric Encryption Keys (public data): E
TPM2_ECDH_KeyGen	Ephemeral key pair generation and Shared Secret Calculation.	'01'	Key handle	zPoint, public point	ECDSA KeyGen	Unauthenticated - Ephemeral User ECC Keys: G
TPM2_ECDH_Zgen	Shared Secret Calculation.	'01'	Key handle, public point	Output point	KAS- ECC- SSC	Object User - Ephemeral User ECC Keys: W,E - TPM ECDH Shared Secret: G
TPM2_ECC_Parameters	Returns the parameters of an ECC curve identified by its TCG-assigned curveID.	'00'	Curve id	ECC parameters for selected curve	None	Unauthenticated
TPM2_EncryptDecrypt	Symmetric encryption or decryption of user data.	'01'	Key handle, encrypt/decrypt, mode, IV, ciphertext/plaintext	Plaintext/ciphertext, IV	AES- CFB128 AES- CTR AES- OFB	Object User - Symmetric Encryption Keys (authValue): E - Symmetric Encryption Keys

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(seedValue): E - Symmetric Encryption Keys (sensitive data): E
TPM2_EncryptDecrypt2	Symmetric encryption or decryption of user data.	'01'	Key handle, encrypt/decrypt, mode, IV, ciphertext/plaintext	Plaintext/ciphertext, IV	AES-CFB128 AES-CTR AES-OFB	Object User - Symmetric Encryption Keys (authValue): E - Symmetric Encryption Keys (seedValue): E - Symmetric Encryption Keys (sensitive data): E
TPM2_Hash	Performs a hash operation on user data.	'01'	Data, hash algorithm, hierarchy	Digest, validation ticket	HMAC SHA	Unauthenticated - Symmetric Signing Keys (authValue): E - Symmetric Signing Keys (seedValue): E - Symmetric Signing Keys (sensitive data): E
TPM2_HMAC	Performs a HMAC operation on user data.	'01'	Key handle, HMAC data, hash algorithm	Returned HMAC	HMAC	Object User - Symmetric Signing Keys (authValue): E - Symmetric Signing Keys (seedValue): E - Symmetric Signing Keys (sensitive data): E
TPM2_GetRandom	Random number generation.	'01'	Number of bytes requested	Random bytes	CTR_D RBG	Unauthenticated - DRBG state:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,E - DRBG Entropy Input: E - Transient DRBG state: G,E
TPM2_StirRandom	Reseed random number generator.	'01'	Key handle, auth value, hash algorithm	Sequence handle	CTR_DRBG Entropy Source	Unauthenticated - DRBG state: G - Transient DRBG state: G - DRBG Entropy Input: W
TPM2_HMAC_Start	HMAC session start	'01'	Key handle, auth value, algorithms to be used	Sequence handle	HMAC	Object User - Symmetric Signing Keys (authValue): E - Symmetric Signing Keys (seedValue): E - Symmetric Signing Keys (sensitive data): E
TPM2_HashSequenceStart	Hash session start	'01'	Auth value, hash algorithm	Sequence handle	SHA	Unauthenticated
TPM2_SequenceUpdate	Sequence update	'01'	Sequence handle, data to add to hash	N/A	HMAC SHA	Unauthenticated - Symmetric Signing Keys (authValue): E - Symmetric Signing Keys (seedValue): E - Symmetric Signing Keys (sensitive data): E
TPM2_SequenceComplete	Sequence complete	'01'	Sequence handle, data, hierarchy	Returned HMAC or	HMAC SHA	Unauthenticated - Symmetric Signing Keys

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
				message digest, ticket		(authValue): E - Symmetric Signing Keys (seedValue): E - Symmetric Signing Keys (sensitive data): E
TPM2_EventSequenceComplete	Event sequence complete	'01'	Data	List of digests	HMAC SHA	Object User - Symmetric Signing Keys (authValue): E - Symmetric Signing Keys (seedValue): E - Symmetric Signing Keys (sensitive data): E
TPM2_CertifyCreation	Proves the association between an object and its creation data	'01'	Sign handle, object handle, qualifying data, creation hash, scheme, creation ticket	Certify info, signature	ECDSA SigGen HMAC KBKDF RSA SigGen SHA	Object Administrator - shProof: E - Asymmetric Signing Keys (authValue): E - Asymmetric Signing Keys (seedValue): E - Asymmetric Signing Keys (sensitive data): E - Asymmetric Signing Keys (authPolicy): E - Asymmetric Signing Keys (public data): E - Symmetric Signing Keys (authValue): E - Symmetric Signing Keys (seedValue): E - Symmetric Signing Keys (sensitive data): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Object User - shProof: E - Asymmetric Signing Keys (authValue): E - Asymmetric Signing Keys (seedValue): E - Asymmetric Signing Keys (sensitive data): E - Asymmetric Signing Keys (authPolicy): E - Asymmetric Signing Keys (public data): E - Symmetric Signing Keys (authValue): E - Symmetric Signing Keys (seedValue): E - Symmetric Signing Keys (sensitive data): E
TPM2_Quote	Quotes PCR values	'01'	sign handle, qualifying data, scheme, PCR selection	quoted information, signature	ECDSA SigGen HMAC KBKDF RSA SigGen SHA	Object User - Asymmetric Signing Keys (authValue): E - Asymmetric Signing Keys (seedValue): E - Asymmetric Signing Keys (sensitive data): E - Asymmetric Signing Keys (authPolicy): E - Asymmetric Signing Keys (public data): E - Symmetric Signing Keys (authValue): E - Symmetric

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Signing Keys (seedValue): E - Symmetric Signing Keys (sensitive data): E
TPM2_GetSessionAuditDigest	Returns a digital signature of the audit session digest	'01'	Privacy administrator handle, sign handle, session handle, qualifying data, scheme	Audit info, signature	ECDSA SigGen HMAC RSA SigGen SHA	Object User - Asymmetric Signing Keys (authValue): E - Asymmetric Signing Keys (seedValue): E - Asymmetric Signing Keys (sensitive data): E - Asymmetric Signing Keys (authPolicy): E - Asymmetric Signing Keys (public data): E - Symmetric Signing Keys (authValue): E - Symmetric Signing Keys (seedValue): E - Symmetric Signing Keys (sensitive data): E - Session (sessionKey): G,E - Session (symKey): G,E
TPM2_GetCommandAuditDigest	Returns the current value of the command audit digest	'01'	Privacy administrator handle, sign handle, qualifying data, scheme	Audit info, signature	ECDSA SigGen HMAC RSA SigGen SHA	Object User - Asymmetric Signing Keys (authValue): E - Asymmetric Signing Keys (seedValue): E - Asymmetric Signing Keys (sensitive

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						data): E - Asymmetric Signing Keys (authPolicy): E - Asymmetric Signing Keys (public data): E - Symmetric Signing Keys (authValue): E - Symmetric Signing Keys (seedValue): E - Symmetric Signing Keys (sensitive data): E
TPM2_GetTime	Returns the current values of Time and Clock	'01'	Privacy administrator handle, sign handle, qualifying data, scheme	Time info, signature	ECDSA SigGen HMAC RSA SigGen SHA	Object User - Asymmetric Signing Keys (authValue): E - Asymmetric Signing Keys (seedValue): E - Asymmetric Signing Keys (sensitive data): E - Asymmetric Signing Keys (authPolicy): E - Asymmetric Signing Keys (public data): E - Symmetric Signing Keys (authValue): E - Symmetric Signing Keys (seedValue): E - Symmetric Signing Keys (sensitive data): E - shProof: E - endorsementAuth: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
TPM2_Sign	Causes the TPM to sign an externally provided hash with the specified symmetric or asymmetric signing key.	'01'	Key handle, digest, scheme, validation	Signature	HMAC RSA SigGen Primitive ECDSA SigGen Component	Object User - Asymmetric Signing Keys (authValue): E - Asymmetric Signing Keys (seedValue): E - Asymmetric Signing Keys (sensitive data): E - Asymmetric Signing Keys (authPolicy): E - Asymmetric Signing Keys (public data): E - Symmetric Signing Keys (authValue): E - Symmetric Signing Keys (seedValue): E - Symmetric Signing Keys (sensitive data): E
TPM2_SetCommandCodeAuditStatus	Used by the Privacy Administrator or platform to change the audit status of a command or to set the hash algorithm used for the audit digest, but not both at the same time.	'00'	Auth handle, hash algorithm, list of commands to be audited, list of commands to no longer be audited	N/A	None	Object User
TPM2_PCR_Extend	Updates the indicated PCR	'01'	PCR handle, digests	N/A	SHA	Object User
TPM2_PCR_Event	Updates the indicated PCR and reports a list of digests	'01'	PCR handle, event data	Digests	SHA	Object User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
TPM2_PCR_Read	Returns the values of all PCR specified in pcrSelectionIn.	'00'	PCT section to read	PCR update counter, returned PCR section, PCR values	None	Unauthenticated
TPM2_PCR_Allocate	Used to set the desired PCR allocation of PCR and algorithms. Requires Platform Authorization.	'00'	Auth handle, PCR allocation selection	Allocation success, max number of PCR, size needed, size available	None	Object User - platformAuth: E
TPM2_PCR_SetAuthPolicy	Used to associate a policy with a PCR or group of PCRs. The policy determines the conditions under which a PCR may be extended or reset.	'00'	Auth handle, auth policy, hash algorithm	N/A	None	Object User - platformAuth: E
TPM2_PCR_SetAuthValue	Changes the authValue of a PCR or group of PCRs.	'00'	PCR handle, auth value	N/A	None	Object User
TPM2_PCR_Reset	Used to set the PCR in all banks to zero.	'00'	PCR handle	N/A	None	Object User
TPM2_PolicySigned	Policy based on signing key	'01'	Signing key handle, policy session handle, TPM nonce, command parameter digest, policy reference, expiration, signed authorization	Timeout, policy ticket	ECDSA SigVer ECDSA SigVer (legacy) HMAC RSA SigVer RSA SigVer (legacy) SHA	Unauthenticated - phProof: E - ehProof: E - shProof: E - nullProof: E - Session (sessionKey): E - Asymmetric Signing Keys (authValue): E - Asymmetric Signing Keys (seedValue): E - Asymmetric Signing Keys (sensitive data): E - Asymmetric Signing Keys (authPolicy): E - Symmetric

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Signing Keys (authValue): E - Symmetric Signing Keys (seedValue): E - Symmetric Signing Keys (sensitive data): E
TPM2_PolicySecret	Policy based on an entity's authValue	'01'	Auth handle, policy session handle, TPM nonce, command parameter digest, policy reference, expiration, signed authorization	Timeout, policy ticket	HMAC SHA	Object User - phProof: E - ehProof: E - shProof: E - nullProof: E
TPM2_PolicyTicket	Policy based on ticket (produced by PolicySigned or PolicySecret)	'01'	Policy session handle, TPM nonce, command parameter digest, policy reference, auth name, ticket	N/A	HMAC SHA	Unauthenticated - phProof: E - ehProof: E - shProof: E - nullProof: E - Session (sessionKey): E
TPM2_PolicyOR	Policy enabling multiple authentication options	'01'	Policy session handle, list of hash values	N/A	SHA	Unauthenticated
TPM2_PolicyPCR	Policy based on PCR	'01'	Policy session handle, PCR digest, PCRs to include the digest	N/A	SHA	Unauthenticated
TPM2_PolicyLocality	Policy based on Locality	'01'	Policy session handle, allowed localities for the policy	N/A	SHA	Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
TPM2_PolicyNV	Policy based on contents of an NV Index	'01'	Auth handle, nv index, policy session handle, operand B, offset of NV index for the start of operand A, operation	N/A	SHA	Object User
TPM2_PolicyCounterTimer	Policy based on time	'01'	Policy session handle, operand B, offset of TPMS_TIME_INFO for operand A, operation	N/A	SHA	Unauthenticated
TPM2_PolicyCommandCode	Policy based on command code	'01'	Policy session handle, command code	N/A	SHA	Unauthenticated
TPM2_PolicyCpHash	Policy bound to specific command with specific parameters and specific objects	'01'	Policy session handle, cpHash	N/A	SHA	Unauthenticated
TPM2_PolicyNameHash	Policy bound to specific objects	'01'	Policy session handle, digest to be added to the policy	N/A	SHA	Unauthenticated
TPM2_PolicyDuplicationSelect	Policy limiting duplication to only a selected parent	'01'	Policy session handle, object name, new parent name, included object name	N/A	SHA	Unauthenticated
TPM2_PolicyAuthorize	Policy enabling policy to change	'01'	Policy Session, digest of	N/A	HMAC SHA	Unauthenticated - Session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			policy being approved, signing key, ticket			(sessionKey): E
TPM2_PolicyAuthValue	Policy bound to authValue of authorized entity (requiring HMAC session)	'01'	Policy session handle	N/A	SHA	Unauthenticated
TPM2_PolicyPassword	Policy bound to authValue of authorized entity (requiring password session)	'01'	Policy session handle	N/A	SHA	Unauthenticated
TPM2_PolicyGetDigest	Returns the current policyDigest of the session.	'00'	Policy session handle	Policy digest	None	Unauthenticated
TPM2_PolicyNvWritten	Policy based on WRITTEN attribute of NV Index	'01'	Policy session handle	Policy digest	SHA	Unauthenticated
TPM2_PolicyTemplate	Policy bound to specific creation template	'01'	Policy session handle, indication whether NV index is required to be written	N/A	SHA	Unauthenticated
TPM2_PolicyAuthorizeNV	Policy bound to policy stored in an NV Index	'01'	Auth handle, nv index, policy session handle	N/A	SHA	Object User
TPM2_CreatePrimary	Creates a Primary Object	'01'	Primary handle, sensitive data, data to provide verifiable linkage between object and owner data, creation PCR	Object handle, public portion, creation data, creation hash, creation ticket, name	CTR_D RBG Entropy Source ECDSA KeyGen HMAC RSA KeyGen SHA AES key generation	Object User - ppSeed: E - epSeed: E - spSeed: E - nullSeed: E - platformAuth: E - endorsementAuth: E - ownerAuth: E - Endorsement Keys (private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					HMAC key generation	values): R - Asymmetric Signing Keys (authValue): G,W - Asymmetric Signing Keys (seedValue): G,W - Asymmetric Signing Keys (sensitive data): G,W - Asymmetric Signing Keys (authPolicy): G,W - Asymmetric Signing Keys (public data): G,W - Asymmetric Encryption Keys (authValue): G,W - Asymmetric Encryption Keys (seedValue): G,W - Asymmetric Encryption Keys (sensitive data): G,W - Asymmetric Encryption Keys (authPolicy): G,W - Asymmetric Encryption Keys (public data): G,W - Symmetric Encryption Keys (authValue): G,W - Symmetric Encryption Keys (seedValue): G,W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Symmetric Encryption Keys (sensitive data): G,W - Symmetric Signing Keys (authValue): G,W - Symmetric Signing Keys (seedValue): G,W - Symmetric Signing Keys (sensitive data): G,W - Object Ephemeral Keys (symKey): G,W,E - Object Ephemeral Keys (hmacKey): G,W,E - DRBG state: G - Transient DRBG state: G - DRBG Entropy Input: W
TPM2_HierarchyControl	Returns the current policyDigest of the session.	'00'	Auth handle, the enable being modified, state	N/A	None	Object User - platformAuth: E - endorsementAuth: E - ownerAuth: E - Asymmetric Signing Keys (authValue): Z - Asymmetric Signing Keys (seedValue): Z - Asymmetric Signing Keys (sensitive data): Z - Asymmetric

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Signing Keys (authPolicy): Z - Asymmetric Signing Keys (public data): Z - Asymmetric Encryption Keys (authValue): Z - Asymmetric Encryption Keys (seedValue): Z - Asymmetric Encryption Keys (sensitive data): Z - Asymmetric Encryption Keys (authPolicy): Z - Asymmetric Encryption Keys (public data): Z - Symmetric Encryption Keys (authValue): Z - Symmetric Encryption Keys (seedValue): Z - Symmetric Encryption Keys (sensitive data): Z - Symmetric Signing Keys (authValue): Z - Symmetric Signing Keys (seedValue): Z - Symmetric Signing Keys (sensitive data): Z
TPM2_SetPrimaryPolicy	Allows setting of the authorization policy for the lockout (lockoutPolicy), the	'00'	Auth handle, auth policy,	N/A	None	Object User - platformAuth: E -

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	platform hierarchy (platformPolicy), the storage hierarchy (ownerPolicy), and the endorsement hierarchy (endorsementPolicy)		hash algorithm			endorsementAuth: E - ownerAuth: E - lockoutAuth: E - platformPolicy: G
TPM2_ChangePPS	Changes the current platform primary seed (PPS)	'01'	Auth handle	N/A	CTR_D RBG	Object User - platformPolicy: E - ppSeed: G,Z - phProof: G,Z - Asymmetric Signing Keys (authValue): Z - Asymmetric Signing Keys (seedValue): Z - Asymmetric Signing Keys (sensitive data): Z - Asymmetric Signing Keys (authPolicy): Z - Asymmetric Signing Keys (public data): Z - Asymmetric Encryption Keys (authValue): Z - Asymmetric Encryption Keys (seedValue): Z - Asymmetric Encryption Keys (sensitive data): Z - Asymmetric Encryption Keys (authPolicy): Z - Asymmetric Encryption Keys (public data): Z - Symmetric

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption Keys (authValue): Z - Symmetric Encryption Keys (seedValue): Z - Symmetric Encryption Keys (sensitive data): Z - Symmetric Signing Keys (authValue): Z - Symmetric Signing Keys (seedValue): Z - Symmetric Signing Keys (sensitive data): Z - DRBG state: G - Transient DRBG state: G - DRBG Entropy Input: W
TPM2_ChangeEPS	Changes the current endorsement primary seed (EPS)	'01'	Auth handle	N/A	CTR_DRBG	Object User - platformPolicy: E - epSeed: G,Z - ehProof: G,Z - endorsementAuth: Z - Asymmetric Signing Keys (authValue): Z - Asymmetric Signing Keys (seedValue): Z - Asymmetric Signing Keys (sensitive data): Z - Asymmetric Signing Keys (authPolicy): Z - Asymmetric Signing Keys

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(public data): Z - Asymmetric Encryption Keys (authValue): Z - Asymmetric Encryption Keys (seedValue): Z - Asymmetric Encryption Keys (sensitive data): Z - Asymmetric Encryption Keys (authPolicy): Z - Asymmetric Encryption Keys (public data): Z - Symmetric Encryption Keys (authValue): Z - Symmetric Encryption Keys (seedValue): Z - Symmetric Encryption Keys (sensitive data): Z - Symmetric Signing Keys (authValue): Z - Symmetric Signing Keys (seedValue): Z - Symmetric Signing Keys (sensitive data): Z - DRBG state: G - Transient DRBG state: G - DRBG Entropy Input: W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
TPM2_Clear	Removes all TPM context associated with a specific Owner.	'01'	Auth handle	N/A	CTR_DRBG	Object User - platformAuth: E - lockoutAuth: E,Z - spSeed: G,Z - shProof: G,Z - ehProof: G,Z - endorsementAuth: Z - ownerAuth: Z - endorsementPolicy: Z - ownerPolicy: Z - lockoutPolicy: Z - NV Index (authValue): Z - NV Index (authPolicy): Z - DRBG state: G - Transient DRBG state: G - DRBG Entropy Input: W
TPM2_ClearControl	Disables and enables the execution of TPM2_Clear().	'00'	Auth handle, disable flag	N/A	None	Object User - platformAuth: E - lockoutAuth: E
TPM2_HierarchyChangeAuth	Allows the authorization secret for a hierarchy or lockout to be changed using the current authorization value as the command authorization.	'00'	Auth handle, new auth value	N/A	None	Object User - platformAuth: E - endorsementAuth: E - ownerAuth: E - lockoutAuth: E
TPM2_DictionaryAttackLockReset	Cancels the effect of a TPM lockout due to a number of successive	'00'	Lock handle	N/A	None	Object User - lockoutAuth: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	authorization failures.					
TPM2_DictionaryAttackParameters	Changes the lockout parameters.	'00'	Lock handle, max tries, recovery time before failure count increases, lockout recovery time	N/A	None	Object User - lockoutAuth: E
TPM2_ContextSave	Save a (object, object sequence or session) context	'01'	Save handle	Context	KBKDF KTS (AES + HMAC) key unwrap ping	Unauthenticated - phProof: E - Context Ephemeral Keys (symKey): G,E - Context Ephemeral Keys (hmacKey): G,E - Session (salt): R
TPM2_ContextLoad	Reload a context	'01'	Context	Loaded handle	KBKDF KTS (AES + HMAC) key wrapping	Unauthenticated - phProof: E - Context Ephemeral Keys (symKey): G,E - Context Ephemeral Keys (hmacKey): G,E - Session (salt): R
TPM2_FlushContext	Causes all context associated with a loaded object, sequence object, or session to be removed from TPM memory.	'00'	Item to flush	N/A	None	Unauthenticated - Session (sessionKey): Z - Asymmetric Signing Keys (authValue): Z
TPM2_EvictControl	Allows certain Transient Objects to	'00'	Auth handle, object	N/A	None	Object User - platformAuth:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	be made persistent or a persistent object to be evicted.		handle, persistent handle			E - ownerAuth: E - Asymmetric Signing Keys (authValue): W - Asymmetric Signing Keys (seedValue): W - Asymmetric Signing Keys (sensitive data): W - Asymmetric Signing Keys (authPolicy): W - Asymmetric Signing Keys (public data): W - Asymmetric Encryption Keys (authValue): W - Asymmetric Encryption Keys (seedValue): W - Asymmetric Encryption Keys (sensitive data): W - Asymmetric Encryption Keys (authPolicy): W - Asymmetric Encryption Keys (public data): W - Symmetric Encryption Keys (authValue): W - Symmetric Encryption Keys

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(seedValue): W - Symmetric Encryption Keys (sensitive data): W - Symmetric Signing Keys (authValue): W - Symmetric Signing Keys (seedValue): W - Symmetric Signing Keys (sensitive data): W
TPM2_ReadClock	Reads the current TPMS_TIME_INFO structure that contains the current setting of Time, Clock, resetCount, and restartCount.	'00'	N/A	Current time	None	Unauthenticated
TPM2_ClockSet	Used to advance the value of the TPM's Clock.	'00'	Auth handle, New time to set	N/A	None	Object User - platformAuth: E - ownerAuth: E
TPM2_ClockRateAdjust	Adjusts the rate of advance of Clock and Time to provide a better approximation to real time.	'00'	Auth handle, rate adjustment	N/A	None	Object User - platformAuth: E - ownerAuth: E
TPM2_GetCapability (Show Version)	Shows status information regarding the TPM and its current state. This can also be used to return firmware version information.	'00'	Property to be read	Returned information.	None	Unauthenticated
Get Device ID (Show hardware identifier)	Used to return hardware version information.	'00'	Device ID register address	0x00FC.	None	Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
TPM2_TestParms	Used to check to see if specific combinations of algorithm parameters are supported.	'00'	Parameters	Success or error	None	Unauthenticated
TPM2_NV_DefineSpace	Defines the attributes of an NV Index and causes the TPM to reserve space to hold the data associated with the NV Index.	'00'	Auth handle, auth value, public parameters of the NV area auth handle, auth value, public parameters of the NV area	N/A	None	Object User - platformAuth: E - ownerAuth: E - NV Index (authValue): G - NV Index (authPolicy): G - Endorsement Keys (public values): E
TPM2_NV_UndefineSpace	Removes an Index from the TPM.	'00'	Auth handle, NV index	N/A	None	Object User - platformAuth: E - ownerAuth: E - NV Index (authValue): Z - NV Index (authPolicy): Z
TPM2_NV_UndefineSpaceSpecial	Allows removal of a platform-created NV Index that has TPMA_NV_POLICY_DELETE SET .	'00'	NV index, platform	N/A	None	Object Administrator - platformAuth: E - ownerAuth: E - NV Index (authValue): Z - NV Index (authPolicy): Z Object User - platformAuth: E - ownerAuth: E - NV Index (authValue): Z - NV Index (authPolicy): Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
TPM2_NV_ReadPublic	Read public area and name of an NV Index	'01'	NV index	NV public area, NV name	SHA	Unauthenticated
TPM2_NV_Write	Writes a value to an area in NV memory that was previously defined by TPM2_NV_DefineSpace().	'00'	Auth handle, nv index, data to write, offset	N/A	None	Object User
TPM2_NV_Increment	Used to increment the value in an NV Index that has the TPM_NT_COUNTER attribute. The data value of the NV Index is incremented by one.	'00'	auth handle, NV index	N/A	None	Object User
TPM2_NV_Extend	Extend data to an NV Index	'01'	auth handle, nv index, data	N/A	SHA	Object User
TPM2_NV_SetBits	Used to SET bits in an NV Index that was created as a bit field.	'00'	auth handle, NV index, bits	N/A	None	Object User
TPM2_NV_WriteLock	If the TPMA_NV_WRITEDEFINE or TPMA_NV_WRITE_STCLEAR attributes of an NV location are SET, then this service may be used to inhibit further writes of the NV Index.	'00'	Auth handle, nv index	N/A	None	Object User
TPM2_NV_GlobalWriteLock	Will SET TPMA_NV_WRITELOCKED for all indexes that have their TPMA_NV_GLOBAL_LOCK attribute SET.	'00'	Auth handle	N/A	None	Object User - platformAuth: E - ownerAuth: E
TPM2_NV_Read	Reads a value from an area in NV memory previously defined by	'00'	Auth handle, nv index, number of	Data	None	Object User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	TPM2_NV_DefineSpace().		octets to read, offset			
TPM2_NV_ReadLock	If TPMA_NV_READ_STCLEAR is SET in an Index, then this service may be used to prevent further reads of the NV Index until the next TPM2_Startup (TPM_SU_CLEAR).	'00'	Auth handle, nv index	N/A	None	Object User
TPM2_NV_ChangeAuth	Allows the authorization secret for an NV Index to be changed.	'00'	NV index, new auth value	N/A	None	Object Administrator - NV Index (authValue): W - NV Index (authPolicy): W
TPM2_NV_Certify	Certify contents of an NV Index.	'01'	Qualifying data, scheme, size, offset	Certify info, signature	ECDSA SigGen HMAC RSA SigGen SHA	Object User - Asymmetric Signing Keys (authValue): E - Asymmetric Signing Keys (seedValue): E - Asymmetric Signing Keys (sensitive data): E - Asymmetric Signing Keys (authPolicy): E - Asymmetric Signing Keys (public data): E - Symmetric Signing Keys (authValue): E - Symmetric Signing Keys (seedValue): E - Symmetric Signing Keys (sensitive data): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
TPM2_ACT_SetTimeout	Used to set the time remaining before an Authenticated Countdown Timer (ACT) expires.	'00'	Act handle, start timeout value	N/A	None	Object User
NTC_FIELD_UPGRADE	Used to verify arguments and protect the input firmware payload	'01'	Firmware payload	N/A	AES-CTR ECDSA SigVer ECDSA SigVer (legacy)	Object Administrator - Firmware Update Keys (ECC): E - Firmware Update Keys (AES): E
SPDM Session Establish	Establish SPDM session. Once SPDM session is established, all TPM commands except TPM2_GetCapability, TPM2_GetTestResult and NTC_FIELD_UPGRADE must be encrypted using either ReqEncKey or RspEncKey.	'01'	sessionID, requestor's ECDH public key, signed transcript hash, HMAC of transcript hash	reqHandshake Secret, rspHandshake Secret, ReqEncKey, RspEncKey, finished_key	CTR_D RBG ECDSA KeyGen ECDSA SigVer HMAC KAS-ECC-SSC HKDF AES-GCM KAS-ECC-SSC + HKDF	Object Administrator - SPDM ECDH Shared Secret: G,E - PSK: E - reqHandshake Secret: G,E,Z - RspEncKey: G,Z - DRBG state: W,E - finished_key: E - ReqEncKey: Z - requester identity signature verification private key: E - responder identity signature verification public key: W,E - rspHandshake Secret: G,E,Z
SPDM PSK Clear	Zeroize PSK	'01'	none	none	SHA	Object Administrator - PSK: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
SPDM PSK Set	Stores encrypted PSK in NV Flash	'01'	PSK	none	AES-CTR	Object Administrator - PSK: R
SPDM Get Public Key	generates new ECDSA pair for SPDM session establishment and outputs public key	'01'	none	ECDSA public key	ECDSA KeyGen	Object Administrator - requester identity signature verification public key: G,R - requester identity signature verification private key: G
SPDM Get Version	returns SPDM protocol version and starts a session and/or clears the existing session if exists	'00'	none	none	None	Object Administrator - ReqEncKey: Z - RspEncKey: Z
SPDM Give Public Key	store requester identity pub key used to verify finishReq->Signature (SPDM encrypted)	'01'	requester identity signature verification public key	none	SHA	Object Administrator - requester identity signature verification public key: W

Table 12: Approved Services

#### 4.4 Non-Approved Services

Name	Description	Algorithms	Role
TPM2_Create	Creation of an ordinary object	CKG	Object User
TPM2_Load	Loading an protected object	KAS-ECC-SSC	Object User
TPM2_LoadExternal	Loading an external object	KAS-ECC-SSC	None
TPM2_CreateLoaded	Creation and loading of an ordinary or a derived object	CKG	Object User
TPM2_RSA_Encrypt	RSA Encryption	RSA Key Transport	None

Name	Description	Algorithms	Role
TPM2_RSA_Decrypt	RSA Decryption	RSA Key Transport	Object User
TPM2_ECDH_ZGen	Shared Secret Calculation with TPM static key and provided public key (1e,1s)	KAS-ECC-SSC	Object User
TPM2_ZGen_2Phase	Ephemeral key pair derivation and Shared Secret Calculation with TPM ephemeral and static key and provided ephemeral and static key (2e,2s)	KAS-ECC-SSC	Object User
TPM2_HMAC	Performs a HMAC operation on user data	HMAC	Object User
TPM2_HMAC_Start	HMAC session start	HMAC	Object User
TPM2_SequenceUpdate	Sequence update	HMAC	Object User
TPM2_SequenceComplete	Sequence complete	HMAC	Object User
TPM2_EventSequenceComplete	Event sequence complete	HMAC	Object User
TPM2_Certify	Proves that an object with a specific Name is loaded in the TPM	RSA signature generation using SHA-1 ECDSA signature generation using SHA-1 HMAC	Object Administrator, Object User
TPM2_CertifyCreation	Proves the association between an object and its creation data	RSA signature generation using SHA-1 ECDSA signature generation using SHA-1 HMAC	Object Administrator, Object User
TPM2_Quote	Quotes PCR values	RSA signature generation using SHA-1 ECDSA signature generation using SHA-1 HMAC	Object User
TPM2_GetSessionAuditDigest	Returns a digital signature of the audit session digest	RSA signature generation using SHA-1 ECDSA signature generation using SHA-1 HMAC	Object User

Name	Description	Algorithms	Role
TPM2_GetCommandAuditDigest	Returns the current value of the command audit digest	RSA signature generation using SHA-1 ECDSA signature generation using SHA-1 HMAC	Object User
TPM2_GetTime	Returns the current values of Time and Clock	RSA signature generation using SHA-1 ECDSA signature generation using SHA-1 HMAC	Object User
TPM2_EC_Ephemeral	Ephemeral key pair derivation	KAS-ECC-SSC	None
TPM2_VerifySignature	Uses loaded keys to validate a signature on a message with the message digest passed to the TPM.	HMAC	None
TPM2_Sign	Causes the TPM to sign an externally provided hash with the specified symmetric or asymmetric signing key.	RSA signature generation using SHA-1 ECDSA signature generation using SHA-1	Object User
TPM2_PolicySigned	Policy based on signing key	ECDSA signature verification component	None
TPM2_PolicySecret	Policy based on an entity's authValue	HMAC	Object User
TPM2_PolicyTicket	Policy based on ticket (produced by PolicySigned or PolicySecret)	HMAC	None
TPM2_PolicyAuthorize	Policy enabling policy to change	HMAC	None
TPM2_CreatePrimary	Creates a Primary Object	CKG	Object User
TPM2_NV_Certify	Certify contents of an NV Index	RSA signature generation using SHA-1 ECDSA signature generation using SHA-1	Object User

Table 13: Non-Approved Services

## 4.5 External Software/Firmware Loaded

The module when operational does not allow loading of external firmware, therefore the firmware load test is not applicable. However, the module offers a firmware upgrade service. Please refer to section 11.2 for details.

## 5 Software/Firmware Security

### 5.1 Integrity Techniques

The integrity of the module is verified by comparing an HMAC-SHA-256 value calculated at run time with stored value calculated during manufacturing.

### 5.2 Initiate on Demand

On demand integrity test may be performed by power cycling.

## 6 Operational Environment

### 6.1 Operational Environment Type and Requirements

The module operates in a limited operational environment per FIPS 140-3 security level 1 specifications.

**Type of Operational Environment:** Limited

## 7 Physical Security

The TPM is implemented as a single integrated circuit (IC) device that attaches to standard system PCBs. It is manufactured using de-facto standard integrated circuit manufacturing technologies, producing a device that meets all commercial-grade power, temperature, reliability, shock and vibration specifications. The TPM IC physical package provides hardness, opacity and tamper-evidence protection conforming to FIPS 140-3 Physical Security Level 3. The TPM achieves this level of protection by implementing an enclosure that is both hard and opaque, as shown in the figures in Section 1. This type of IC package ensures that any physical tampering will always result in scratches, chipping, or other visible damage on the enclosure. Before the TPM is integrated into a target application system, it must be checked visually for tampering. After it is integrated, typically through soldering onto a PCB, it can be inspected for tampering by opening the application system enclosure and examining the TPM.

### 7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Hard tamper-evident coating	Determined by the operator	Observe the coating surrounding the chip for any signs of damage

Table 14: Mechanisms and Actions Required

### 7.2 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-197.9°C	EFT	The module remained operational without producing errors
HighTemperature	200.4°C	EFT	The module remained operational without producing errors
LowVoltage	1.7V	EFT	Module shuts down
HighVoltage	3.47V	EFT	Module shuts down

Table 15: EFP/EFT Information

### 7.3 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-40°C
HighTemperature	105°C

Table 16: Hardness Testing Temperatures

## 8 Non-Invasive Security

This module does not implement any non-invasive security mechanism defined in SP800-140F, therefore this section is not applicable.

## 9 Sensitive Security Parameters Management

### 9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Flash	Storage location for firmware components and persistent SSPs.	Static
RAM	Storage location for runtime operations and transient SSPs.	Dynamic
Stack	Storage location for ephemeral keys.	Dynamic

Table 17: Storage Areas

### 9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
TPM2_Load	Entity using the module	RAM	Encrypted	Manual	Electronic	KTS (AES + HMAC) key unwrapping
TPM2_EvictControl	Entity using the module	RAM	Encrypted	Manual	Electronic	KTS (AES + HMAC) key unwrapping
TPM2_Import	Entity using the module	RAM	Encrypted	Manual	Electronic	KTS (AES + HMAC) key unwrapping
TPM2_Create (Import)	Entity using the module	RAM	Encrypted	Manual	Electronic	KTS (AES + HMAC) key unwrapping
TPM2_Create (Export)	RAM	Entity using the module	Encrypted	Manual	Electronic	KTS (AES + HMAC) key wrapping
TPM2_CreatePrimary (Import)	Entity using the module	RAM	Encrypted	Manual	Electronic	KTS (AES + HMAC) key unwrapping
TPM2_CreatePrimary (Export)	RAM	Entity using the module	Encrypted	Manual	Electronic	KTS (AES + HMAC) key wrapping
TPM2_CreateLoaded	RAM	Entity using the module	Encrypted	Manual	Electronic	KTS (AES + HMAC) key wrapping

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
TPM2_ContextLoad	RAM	Entity using the module	Encrypted	Manual	Electronic	KTS (AES + HMAC) key wrapping
TPM2_ContextSave	Entity using the module	RAM	Encrypted	Manual	Electronic	KTS (AES + HMAC) key unwrapping
TPM2_ReadPublic	RAM	Entity using the module	Encrypted	Manual	Electronic	KTS (AES + HMAC) key wrapping
TPM2_ObjectChangeAuth (Import)	Entity using the module	RAM	Encrypted	Manual	Electronic	KTS (AES + HMAC) key unwrapping
TPM2_ObjectChangeAuth (Export)	RAM	Entity using the module	Encrypted	Manual	Electronic	KTS (AES + HMAC) key wrapping
TPM2_NV_ChangeAuth (Import)	Entity using the module	RAM	Encrypted	Manual	Electronic	KTS (AES + HMAC) key unwrapping
TPM2_NV_ChangeAuth (Export)	RAM	Entity using the module	Encrypted	Manual	Electronic	KTS (AES + HMAC) key wrapping
TPM2_Rewrap (Import) (Symmetric Operation)	Entity using the module	RAM	Encrypted	Manual	Electronic	KTS (AES + HMAC) key unwrapping
TPM2_Rewrap (Import) (Asymmetric Operation)	Entity using the module	RAM	Encrypted	Manual	Electronic	KTS RSA
TPM2_Rewrap (Export) (Symmetric Operation)	RAM	Entity using the module	Encrypted	Manual	Electronic	KTS (AES + HMAC) key wrapping
TPM2_Rewrap (Export) (Asymmetric Operation)	RAM	Entity using the module	Encrypted	Manual	Electronic	KTS RSA
TPM2_HierarchyChangeAuth	Entity using the module	RAM	Encrypted	Manual	Electronic	KTS (AES + HMAC) key unwrapping
TPM2_SetPrimaryPolicy	Entity using the module	RAM	Encrypted	Manual	Electronic	KTS (AES + HMAC) key unwrapping

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
TPM2_Duplicate (Import, Plain)	Entity using the module	RAM	Plaintext	Manual	Electronic	
TPM2_Duplicate (Import, Encrypted) (Symmetric Operation)	Entity using the module	RAM	Encrypted	Manual	Electronic	KTS (AES + HMAC) key unwrapping
TPM2_Duplicate (Import, Encrypted) (Asymmetric Operation)	Entity using the module	RAM	Encrypted	Manual	Electronic	KTS RSA
TPM2_Duplicate (Export, Plain)	RAM	Entity using the module	Plaintext	Manual	Electronic	
TPM2_Duplicate (Export, Encrypted) (Symmetric Operation)	RAM	Entity using the module	Encrypted	Manual	Electronic	KTS (AES + HMAC) key wrapping
TPM2_Duplicate (Export, Encrypted) (Asymmetric Operation)	RAM	Entity using the module	Encrypted	Manual	Electronic	KTS RSA
TPM2_LoadExternal	Entity using the module	RAM	Plaintext	Manual	Electronic	
TPM2_MakeCredential	Entity using the module	RAM	Encrypted	Manual	Electronic	KTS RSA
TPM2_ActivateCredential	RAM	Entity using the module	Encrypted	Manual	Electronic	KTS RSA
SPDM Session Establish	Entity using the module	RAM	Plaintext	Manual	Electronic	

Table 18: SSP Input-Output Methods

The module requires two independent internal actions to output SSP in plaintext. The TPM2\_Duplicate command performs the following actions:

- 1) Verification of the encryptedDuplication attribute of the key to be duplicated: encryptedDuplication attribute needs to be set to 0
- 2) Verification of the handle of the new parent of the key to be duplicated: new handle needs to be set to the NULL handle

### 9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Stack Cleaning	Procedurally clears the stack after ephemeral key is no longer needed	Zeroize the stack contents in memory	Automatically by the module
TPM2_Clear	Removes all TPM context associated with a specific Owner	Zeroize objects (overwrites with zeros) in memory and persistent storage. Overwrites spSeed, shProof and ehProof with random data. Zeroize (overwrites with zeros) ownerAuth, ownerPolicy, endorsementAuth, endorsementPolicy, lockoutAuth, lockoutPolicy	By invoking the TPM2_Clear service
TPM2_ChangeEPS	overwrites with random data the current endorsement primary seed (EPS)	epSeed is overwritten by random values from the DRBG. ehProof, endorsementAuth and endorsementPolicy are zeroized. Flushes any resident objects.	By invoking the TPM2_ChangeEPS service
TPM2_ChangePPS	overwrites with random data the current platform primary seed (PPS)	ppSeed is overwritten by random values from the DRBG. platformPolicy is zeroized. Flushes any resident objects.	By invoking the TPM2_ChangePPS service
TPM2_Startup	Can be used to reset the module and have all variables go to the default initialization state	All variables are overwritten back to the default values (zeroed).	By invoking the TPM2_Startup service
TPM2_FlushContext	Causes all context associated with a loaded object, sequence object, or session to be zeroized (overwritten with zeros) from TPM memory.	Clears objects from memory.	By invoking the TPM2_FlushContext service
TPM2_NV_UndefineSpace	Removes an Index from the TPM.	Index is removed from the TPM.	By invoking the TPM2_NV_UndefineSpace service
TPM2_HierarchyControl	This command enables and disables use of a hierarchy and its associated NV storage. The	Zeroizes non-volatile stored values related to the disabled hierarchy	By invoking the TPM2_HierarchyControl service

Zeroization Method	Description	Rationale	Operator Initiation
	command allows phEnable, phEnableNV, shEnable, and ehEnable to be overwritten with random data when the proper authorization is provided.		
Clear TPM	Persistent memory is zeroized using a proprietary method	zeroizes (overwrites with zeros) all module contents	For further information and instructions on clearing the flash, contact the platform manufacturer or Nuvoton support
SPDM session reset	closes out SPDM session, zeroizing all session keys.	zeroizes (overwrites with zeros) SPDM state and session keys	By providing the "GET_VERSION" request code in a TPM command with the SPDM_CLEAR_MESSAGE_TAG
PSK Clear	Zeroizes PSK	Zeroizes (overwrites with zeros) PSK	by invoking SPDM PSK Clear service
TPM2_PolicyRestart	Authorization session variables are zeroized (overwrites with zeros).	All variables are overwritten back to the default values (zeroed).	By invoking the TPM2_PolicyRestart service

Table 19: SSP Zeroization Methods

## 9.4 SSPs

The table below summarizes the Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ppSeed	KBKDF derivation keys to derive primary object's seedValue and sensitive data	512 bits - 512 bits	Seed Value - CSP	CTR_DRBG		KBKDF
epSeed	KBKDF derivation keys to derive primary object's seedValue and sensitive data	512 bits - 512 bits	Seed Value - CSP	CTR_DRBG		KBKDF
spSeed	KBKDF derivation keys to derive primary object's seedValue and sensitive data	512 bits - 512 bits	Seed Value - CSP	CTR_DRBG		KBKDF

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
nullSeed	KBKDF derivation keys to derive primary object's seedValue and sensitive data	512 bits - 512 bits	Seed Value - CSP	CTR_DRBG		KBKDF
phProof	Used as KBKDF derivation key to derive context encryption key. It's also used as a HMAC key to prove that an externally stored computation (context blob or a ticket) was created or checked by the TPM.	512 bits - 512 bits	Proof Values - CSP	CTR_DRBG		KBKDF
ehProof	Used as KBKDF derivation key to derive context encryption key. It's also used as a HMAC key to prove that an externally stored computation (context blob or a ticket) was created or checked by the TPM.	512 bits - 512 bits	Proof Values - CSP	CTR_DRBG		KBKDF
shProof	Used as KBKDF derivation key to derive context encryption key. It's also used as a HMAC key to prove that an externally stored computation (context blob or a ticket) was created or checked by the TPM.	512 bits - 512 bits	Proof Values - CSP	CTR_DRBG		KBKDF
nullProof	Used as KBKDF derivation key to derive context encryption key. It's also used as a HMAC key to prove that an externally stored computation (context blob or a ticket) was created or checked by the TPM.	512 bits - 512 bits	Proof Values - CSP	CTR_DRBG		KBKDF

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
platformAuth	Authorization data known to the hierarchy owner, required when using or changing the Hierarchy in Password or HMAC sessions.	Same as digest - Same as digest	Authorization Values - CSP			
endorsementAuth	Authorization data known to the hierarchy owner, required when using or changing the Hierarchy in Password or HMAC sessions	Same as digest - Same as digest	Authorization Values - CSP			
ownerAuth	Authorization data known to the hierarchy owner, required when using or changing the Hierarchy in Password or HMAC sessions	Same as digest - Same as digest	Authorization Values - CSP			
lockoutAuth	Authorization data known to the hierarchy owner, required when using or changing the Hierarchy in Password or HMAC sessions	Same as digest - Same as digest	Authorization Values - CSP			
platformPolicy	Authorization data known to the hierarchy owner, required when using or changing the Hierarchy in Policy sessions	Same as digest - Same as digest	Policies - CSP			
endorsementPolicy	Authorization data known to the hierarchy owner, required when using or changing the Hierarchy in Policy sessions	Same as digest - Same as digest	Policies - CSP			
ownerPolicy	Authorization data known to the	Same as	Policies - CSP			

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	hierarchy owner, required when using or changing the Hierarchy in Policy sessions	digest - Same as digest				
lockoutPolicy	Authorization data known to the hierarchy owner, required when using or changing the Hierarchy in Policy sessions	Same as digest - Same as digest	Policies - CSP			
Asymmetric Signing Keys (authValue)	Authorization data known to the Object owner, required when using or changing the Asymmetric Signing Key Object.	Same as digest - Same as digest	Object Keys - CSP			
Asymmetric Signing Keys (seedValue)	Unused (set to 0).	Same as digest - Same as digest	Object Keys - CSP		KBKDF	KBKDF
Asymmetric Signing Keys (sensitive data)	ECDSA/RSA Private Data for Signature Generation and Verification (including intermediate keygen values)	ECDSA: P-256, P-384; RSA: 2048, 3072, 4096 - ECDSA: 128 or 192 bits; RSA: 112, 128 or 150 bits	Object Keys - CSP	ECDSA KeyGen RSA KeyGen		ECDSA SigGen RSA SigGen RSA SigGen Primitive
Asymmetric Signing Keys (authPolicy)	Command authentication data	Same as digest - Same as digest	Object Keys - CSP			
Asymmetric Signing Keys (public data)	ECDSA/RSA Public Data	ECDSA: P-256, P-384; RSA:	Object Keys - PSP	ECDSA KeyGen		ECDSA KeyVer ECDSA SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		2048, 3072, 4096 - ECDSA: 128 or 192 bits; RSA: 112, 128 or 150 bits		RSA KeyGen		ECDSA SigVer (legacy) RSA SigVer RSA SigVer (legacy)
Asymmetric Encryption Keys (authValue)	Authorization data known to the Object owner, required when using or changing the Object.	Same as digest - Same as digest	Object Keys - CSP			
Asymmetric Encryption Keys (seedValue)	Authorization data known to the Object owner, required when using or changing the Object.	Same as digest - Same as digest	Object Keys - CSP		KBKDF	KBKDF
Asymmetric Encryption Keys (sensitive data)	ECC/RSA Private Data including intermediate keygen values	ECC: P-256, P-384; RSA: 2048, 3072, 4096 - ECC: 128 or 192 bits; RSA: 112, 128 or 150 bits	Object Keys - CSP	CTR_DRBG ECDSA KeyGen		KAS-ECC KAS-ECC-SSC KTS RSA
Asymmetric Encryption Keys (authPolicy)	Command authentication data	512 bits - 512 bits	Object Keys - CSP			
Asymmetric Encryption Keys (public data)	ECC/RSA Public Data	ECC: P-256, P-384; RSA: 2048, 3072, 4096 - ECC: 128 or	Object Keys - PSP			KAS-ECC KAS-ECC-SSC KTS RSA

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		192 bits; RSA: 112, 128 or 150 bits				
Symmetric Encryption Keys (authValue)	Authorization data known to the Object owner, required when using or changing the Symmetric Encryption Key Object	Same as digest - Same as digest	Object Keys - CSP			
Symmetric Encryption Keys (seedValue)	Used to compute the unique field (If restricted decrypt key - by using HMAC, if not a restricted decrypt key - by hashing with the sensitive field)	Same as digest - Same as digest	Object Keys - CSP			
Symmetric Encryption Keys (sensitive data)	Symmetric encryption using AES	128 or 256 bits - 128 or 256 bits	Object Keys - CSP			AES-CFB128 AES-CTR AES-OFB
Symmetric Signing Keys (authValue)	Authorization data known to the Object owner, required when using or changing the Symmetric Signing Key Object	Same as digest - Same as digest	Object Keys - CSP			
Symmetric Signing Keys (seedValue)	Additionally used to compute the unique field (If restricted decrypt key - by using HMAC, if not a restricted decrypt key - by hashing with the sensitive field)	Same as digest - Same as digest	Object Keys - CSP			
Symmetric Signing Keys (sensitive data)	Message Authentication Code using HMAC	160, 256, 384 bits - 160, 256, 384 bits	Object Keys - CSP			HMAC
Object Ephemeral Keys (symKey)	Symmetric encryption key (AES) protecting	128 or 256 bits	Ephemeral Key Wrapping Keys (Symmetric)		KBKDF	AES-CFB128 KTS (AES + HMAC)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	(encryption) the object sensitive data	- 128 or 256 bits	Encryption/Decryption) - CSP			key wrapping KTS (AES + HMAC) key unwrapping
Object Ephemeral Keys (hmacKey)	Symmetric signing key (HMAC) protecting (integrity) the encrypted data	160, 256, 384 bits - 160, 256, 384 bits	Ephemeral Key Wrapping Keys (MAC) - CSP		KBKDF	HMAC KTS (AES + HMAC) key wrapping KTS (AES + HMAC) key unwrapping
Duplication Ephemeral Keys (symKey)	Symmetric encryption key (AES) protecting (encryption) the object sensitive data	128 or 256 bits - 128 or 256 bits	Ephemeral Key Wrapping Keys (Symmetric Encryption/Decryption) - CSP		KAS-ECC KTS RSA	AES-CFB128 KTS (AES + HMAC) key wrapping KTS (AES + HMAC) key unwrapping
Duplication Ephemeral Keys (hmacKey)	Symmetric signing key (HMAC) protecting (integrity) the encrypted data	160, 256, 384 bits - 160, 256, 384 bits	Ephemeral Key Wrapping Keys (MAC) - CSP		KAS-ECC KTS RSA	HMAC KTS (AES + HMAC) key wrapping KTS (AES + HMAC) key unwrapping
Duplication Ephemeral Keys (innerSymKey)	Symmetric encryption key (AES) for double protecting (encryption) the object sensitive data	128 or 256 bits - 128 or 256 bits	Ephemeral Key Wrapping Keys Ephemeral Key Wrapping Keys (Symmetric Encryption/Decryption) - CSP	CTR_DRBG		AES-CFB128 KTS (AES + HMAC) key wrapping KTS (AES + HMAC) key unwrapping

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Context Ephemeral Keys (symKey)	Symmetric encryption key (AES) protecting (encryption) the the externally stored objects, sequence objects, and sessions	128 or 256 bits - 128 or 256 bits	Ephemeral Key Wrapping Keys Ephemeral Key Wrapping Keys (Symmetric Encryption/Decryption) - CSP		KBKDF	AES-CFB128 KTS (AES + HMAC) key wrapping KTS (AES + HMAC) key unwrapping
Context Ephemeral Keys (hmacKey)	Symmetric signing key (HMAC) protecting (integrity) the encrypted data	160, 256, 384 bits - 160, 256, 384 bits	Ephemeral Key Wrapping Keys (MAC) - CSP		KBKDF	HMAC KTS (AES + HMAC) key wrapping KTS (AES + HMAC) key unwrapping
Credential Ephemeral Keys (symKey)	Symmetric encryption key (AES) protecting (encryption) the the externally stored objects, sequence objects, and sessions	128 or 256 bits - 128 or 256 bits	Ephemeral Key Wrapping Keys (Symmetric Encryption/Decryption) - CSP		KAS-ECC KTS RSA	AES-CFB128 KTS (AES + HMAC) key wrapping KTS (AES + HMAC) key unwrapping
Credential Ephemeral Keys (hmacKey)	Symmetric signing key (HMAC) protecting (integrity) the encrypted data	160, 256, 384 bits - 160, 256, 384 bits	Ephemeral Key Wrapping Keys (MAC) - CSP		KAS-ECC KTS RSA	HMAC KTS (AES + HMAC) key wrapping KTS (AES + HMAC) key unwrapping
Ephemeral Key Agreement Keys	ECC ephemeral keys used in Diffie-Hellman key exchange.	P-256, P-384 - 128 or 192 bits	Asymmetric Ephemeral Keys - CSP	CTR_DRBG ECDSA KeyGen	KBKDF	KAS-ECC
Ephemeral User ECC Keys	ECC private key used for user cryptography support	P-256, P-384 -	Asymmetric Ephemeral Keys - CSP	CTR_DRBG	KBKDF	KAS-ECC-SSC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		128 or 192 bits		ECDSA KeyGen		
Endorsement Keys (private values)	Private key values for Digital Signature Generation/Verification	ECC: P-256, P-384; RSA: 2048, 3072, 4096 - ECC: 128 or 192 bits; RSA: 112, 128 or 150 bits	Endorsement Keys (Asymmetric) - CSP			ECDSA SigGen ECDSA SigVer
Endorsement Keys (public values)	Certificates containing the public RSA\ECC keys	ECC: P-256, P-384; RSA: 2048, 3072, 4096 - ECC: 128 or 192 bits; RSA: 112, 128 or 150 bits	Endorsement Keys (Asymmetric) - PSP			ECDSA SigGen ECDSA SigVer ECDSA SigVer (legacy)
Firmware Update Keys (ECC)	ECC Public Key Used to verify arguments of FU_Start & FU_Complete commands using ECDSA	P-256, P-384 - 128 or 192 bits	Firmware Update Keys - PSP			ECDSA SigVer
Firmware Update Keys (AES)	Used to decrypt input payload of FU_Load command	128 or 256 bits - 128 or 256 bits	Firmware Update Keys - CSP			AES-CTR
NV Index (authValue)	Authorization data used in authorization session, and extended into policyDigest on TPM2_PolicySecret command	Same as digest - Same as digest	NV Index - CSP			

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
NV Index (authPolicy)	Authorization data used in policy session	Same as digest - Same as digest	NV Index - CSP			
Session (salt)	KBKDF derivation key to derive sessionKey	384 bits - 384 bits	Session Keys - CSP			KBKDF
Session (sessionKey)	HMAC key to compute session HMAC	160, 256, 384 bits - 160, 256, 384 bits	Session Keys - CSP		KBKDF	HMAC KBKDF
Session (symKey)	Ephemeral symmetric encryption key for message parameter encrypt/decrypt (of the first sized buffer parameter, if a session-based encryption is used)	128 or 256 bits - 128 or 256 bits	Session Keys - CSP		KBKDF	AES-CFB128 AES-CTR AES-OFB
DRBG state	The CTR DRBG working state. Contains the current V and Key	384 bits - 384 bits	DRBG Keys - CSP			CTR_DRBG
DRBG Entropy Input	Bit stream produced from the entropy source, used as entropy input for the DRBG's seed	256 bits to 2 <sup>32</sup> bits - 256 bits to 2 <sup>32</sup> bits	DRBG Keys - CSP	Entropy Source		CTR_DRBG
Transient DRBG state	Local DRBG state used for pseud-random during CreatePrimary command	384 bits - 384 bits	DRBG Keys - CSP			CTR_DRBG
finished_key	SPDM key used to calculate HMAC of the hash of the concatenation of all messages sent so far between the	384 bits - 384 bits	HMAC key - CSP		HKDF	HMAC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Requester and the Responder					
SPDM ECDH Shared Secret	SPDM key used to derive various encryption keys used by a SPDM session	384 bits - 384 bits	HKDF IKM - CSP		KAS-ECC-SSC	HKDF
reqHandshakeSecret	SPDM Requestor-direction handshake key used to calculate HMAC of the hash of all requests after KEY_EXCHANGE or PSK_EXCHANGE up to and including FINISH or PSK_FINISH	384 bits - 384 bits	HMAC Key - CSP		HKDF	HMAC
rspHandshakeSecret	SPDM Responder-direction handshake key used to calculate HMAC of the hash of all requests after KEY_EXCHANGE_RSP or PSK_EXCHANGE_RSP up to and including FINISH_RSP or PSK_FINISH_RSP	384 bits - 384 bits	HMAC Key - CSP		HKDF	HMAC
ReqEncKey	SPDM Requestor-direction encryption key used to encrypt all data traveling from the Requester to the Responder	256 bits - 256 bits	AES key - CSP		HKDF	AES-GCM
RspEncKey	SPDM Responder-direction encryption key used to encrypt all data traveling from the Responder to the Requester	256 bits - 256 bits	AES key - CSP		HKDF	AES-GCM
PSK	SPDM key used to derive various encryption keys used by a SPDM session	384 bits - 384 bits	HKDF IKM - CSP			HKDF
requester identity signature	requester identity signature verification public key used to	384 bits - 384 bits	ECDSA signature verification key - PSP	ECDSA KeyGen		ECDSA SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
verification public key	verify SPDM finish->SignatureData					
requester identity signature verification private key	requester identity signature private key generated by "SPDM Get Public Key"	384 bits - 384 bits	ECDSA signature generation key - PSP	ECDSA KeyGen		
TPM ECDH Shared Secret	Shared Secret used to derive various encryption keys used by the TPM	128 or 192 bits - 128 or 192 bits	Shared Secret - CSP		KAS-ECC-SSC	KDA
responder identity signature verification public key	responder identity signature public key imported during session establishment	384 bits - 384 bits	ECDSA signature verification key - PSP			ECDSA SigVer

Table 20: SSP Table 1

The following table continues to summarize the Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
ppSeed		Flash:Obfuscated	N/A	TPM2_ChangePPS	
epSeed		Flash:Obfuscated	N/A	TPM2_ChangeEPS	
spSeed		Flash:Obfuscated	N/A	TPM2_Clear	
nullSeed		RAM:Plaintext	Until reset	TPM2_Startup	
phProof		Flash:Obfuscated	N/A	TPM2_ChangePPS	
ehProof		Flash:Obfuscated	N/A	TPM2_Clear TPM2_ChangeEPS	
shProof		Flash:Obfuscated	N/A	TPM2_Clear	
nullProof		RAM:Plaintext	N/A	TPM2_Startup	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
platformAuth	TPM2_HierarchyChangeAuth	RAM:Plaintext	Until reset	TPM2_Startup	
endorsementAuth	TPM2_HierarchyChangeAuth	Flash:Obfuscated	N/A	TPM2_Clear TPM2_ChangeEPS	
ownerAuth	TPM2_HierarchyChangeAuth	Flash:Obfuscated	N/A	TPM2_Clear	
lockoutAuth	TPM2_HierarchyChangeAuth	Flash:Obfuscated	N/A	TPM2_Clear	
platformPolicy	TPM2_SetPrimaryPolicy	RAM:Plaintext	N/A	TPM2_Startup	
endorsementPolicy	TPM2_SetPrimaryPolicy	Flash:Obfuscated	N/A	TPM2_Clear TPM2_ChangeEPS TPM2_Startup	
ownerPolicy	TPM2_SetPrimaryPolicy	Flash:Obfuscated	N/A	TPM2_Clear TPM2_Startup	
lockoutPolicy	TPM2_SetPrimaryPolicy	Flash:Obfuscated	N/A	TPM2_Clear TPM2_Startup	
Asymmetric Signing Keys (authValue)	TPM2_Load TPM2_LoadExternal TPM2_EvictControl TPM2_Create (Import) TPM2_Create (Export) TPM2_CreatePrimary (Import) TPM2_CreatePrimary (Export) TPM2_CreateLoaded TPM2_ReadPublic TPM2_ObjectChangeAuth (Import) TPM2_ObjectChangeAuth (Export) TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation) TPM2_Duplicate (Export, Plain) TPM2_Duplicate (Export, Encrypted) (Symmetric Operation)	RAM:Plaintext Flash:Obfuscated	N/A	TPM2_ChangeEPS TPM2_ChangePPS TPM2_Startup TPM2_FlushContext TPM2_HierarchyControl Clear TPM	Asymmetric Signing Keys (seedValue):Used With Asymmetric Signing Keys (sensitive data):Used With Asymmetric Signing Keys (authPolicy):Used With Asymmetric Signing Keys (public data):Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Asymmetric Signing Keys (seedValue)	TPM2_Load TPM2_LoadExternal TPM2_EvictControl TPM2_Create (Import) TPM2_Create (Export) TPM2_CreatePrimary (Import) TPM2_CreatePrimary (Export) TPM2_CreateLoaded TPM2_ReadPublic TPM2_ObjectChangeAuth (Import) TPM2_ObjectChangeAuth (Export) TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation) TPM2_Duplicate (Export, Plain) TPM2_Duplicate (Export, Encrypted) (Symmetric Operation)	RAM:Plaintext Flash:Obfuscated	N/A	TPM2_ChangeEPS TPM2_ChangePPS TPM2_Startup TPM2_FlushContext TPM2_HierarchyControl Clear TPM	Asymmetric Signing Keys (authValue):Used With Asymmetric Signing Keys (sensitive data):Used With Asymmetric Signing Keys (authPolicy):Used With Asymmetric Signing Keys (public data):Used With ppSeed:Derived From
Asymmetric Signing Keys (sensitive data)	TPM2_Load TPM2_LoadExternal TPM2_EvictControl TPM2_Create (Import) TPM2_Create (Export) TPM2_CreatePrimary (Import) TPM2_CreatePrimary (Export) TPM2_CreateLoaded TPM2_ReadPublic TPM2_ObjectChangeAuth (Import) TPM2_ObjectChangeAuth (Export) TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation) TPM2_Duplicate (Export, Plain) TPM2_Duplicate (Export, Encrypted) (Symmetric Operation)	RAM:Plaintext Flash:Obfuscated	N/A	TPM2_ChangeEPS TPM2_ChangePPS TPM2_Startup TPM2_FlushContext TPM2_HierarchyControl Clear TPM	Asymmetric Signing Keys (authValue):Used With Asymmetric Signing Keys (seedValue):Used With Asymmetric Signing Keys (authPolicy):Used With Asymmetric Signing Keys (public data):Used With ppSeed:Derived From
Asymmetric Signing Keys (authPolicy)	TPM2_Load TPM2_LoadExternal TPM2_EvictControl TPM2_Create (Import)	RAM:Plaintext Flash:Obfuscated	N/A	TPM2_ChangeEPS TPM2_ChangePPS TPM2_Startup TPM2_FlushContext	Asymmetric Signing Keys (authValue):Used With Asymmetric Signing

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	TPM2_Create (Export) TPM2_CreatePrimary (Import) TPM2_CreatePrimary (Export) TPM2_CreateLoaded TPM2_ReadPublic TPM2_ObjectChangeAuth (Import) TPM2_ObjectChangeAuth (Export) TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation) TPM2_Duplicate (Export, Plain) TPM2_Duplicate (Export, Encrypted) (Symmetric Operation)			TPM2_HierarchyControl Clear TPM	Keys (seedValue):Used With Asymmetric Signing Keys (sensitive data):Used With Asymmetric Signing Keys (public data):Used With
Asymmetric Signing Keys (public data)	TPM2_Load TPM2_LoadExternal TPM2_EvictControl TPM2_Create (Import) TPM2_Create (Export) TPM2_CreatePrimary (Import) TPM2_CreatePrimary (Export) TPM2_CreateLoaded TPM2_ReadPublic TPM2_ObjectChangeAuth (Import) TPM2_ObjectChangeAuth (Export) TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation) TPM2_Duplicate (Export, Plain) TPM2_Duplicate (Export, Encrypted) (Symmetric Operation)	RAM:Plaintext Flash:Obfuscated	N/A	TPM2_ChangeEPS TPM2_ChangePPS TPM2_Startup TPM2_FlushContext TPM2_HierarchyControl Clear TPM	Asymmetric Signing Keys (authValue):Used With Asymmetric Signing Keys (seedValue):Used With Asymmetric Signing Keys (sensitive data):Used With Asymmetric Signing Keys (authPolicy):Used With
Asymmetric Encryption Keys (authValue)	TPM2_Load TPM2_LoadExternal TPM2_EvictControl TPM2_Create (Import) TPM2_Create (Export) TPM2_CreatePrimary (Import) TPM2_CreatePrimary (Export)	RAM:Plaintext Flash:Obfuscated	N/A	TPM2_ChangeEPS TPM2_ChangePPS TPM2_Startup TPM2_FlushContext TPM2_HierarchyControl Clear TPM	Asymmetric Encryption Keys (seedValue):Used With Asymmetric Encryption Keys (sensitive data):Used With Asymmetric Encryption Keys (authPolicy):Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	TPM2_CreateLoaded TPM2_ReadPublic TPM2_ObjectChangeAuth (Import) TPM2_ObjectChangeAuth (Export) TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation) TPM2_Duplicate (Export, Plain) TPM2_Duplicate (Export, Encrypted) (Symmetric Operation)				Asymmetric Encryption Keys (public data):Used With Symmetric Encryption Keys (authValue):Used With
Asymmetric Encryption Keys (seedValue)	TPM2_Load TPM2_LoadExternal TPM2_EvictControl TPM2_Create (Import) TPM2_Create (Export) TPM2_CreatePrimary (Import) TPM2_CreatePrimary (Export) TPM2_CreateLoaded TPM2_ReadPublic TPM2_ObjectChangeAuth (Import) TPM2_ObjectChangeAuth (Export) TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation) TPM2_Duplicate (Export, Plain) TPM2_Duplicate (Export, Encrypted) (Symmetric Operation)	RAM:Plaintext Flash:Obfuscated	N/A	TPM2_ChangeEPS TPM2_ChangePPS TPM2_Startup TPM2_FlushContext TPM2_HierarchyControl Clear TPM	Asymmetric Encryption Keys (authValue):Used With Asymmetric Encryption Keys (sensitive data):Used With Asymmetric Encryption Keys (authPolicy):Used With Asymmetric Encryption Keys (public data):Used With Symmetric Encryption Keys (authValue):Used With ppSeed:Derived From
Asymmetric Encryption Keys (sensitive data)	TPM2_Load TPM2_LoadExternal TPM2_EvictControl TPM2_Create (Import) TPM2_Create (Export) TPM2_CreatePrimary (Import) TPM2_CreatePrimary (Export) TPM2_CreateLoaded TPM2_ReadPublic TPM2_ObjectChangeAuth (Import) TPM2_ObjectChangeAuth (Export)	RAM:Plaintext Flash:Obfuscated	N/A	TPM2_ChangeEPS TPM2_ChangePPS TPM2_Startup TPM2_FlushContext TPM2_HierarchyControl Clear TPM	Asymmetric Encryption Keys (authValue):Used With Asymmetric Encryption Keys (seedValue):Used With Asymmetric Encryption Keys (authPolicy):Used With Asymmetric Encryption Keys (public data):Used With Symmetric Encryption Keys (authValue):Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	uth (Export) TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation) TPM2_Duplicate (Export, Plain) TPM2_Duplicate (Export, Encrypted) (Symmetric Operation)				With ppSeed:Derived From
Asymmetric Encryption Keys (authPolicy)	TPM2_Load TPM2_LoadExternal TPM2_EvictControl TPM2_Create (Import) TPM2_Create (Export) TPM2_CreatePrimary (Import) TPM2_CreatePrimary (Export) TPM2_CreateLoaded TPM2_ReadPublic TPM2_ObjectChangeA uth (Import) TPM2_ObjectChangeA uth (Export) TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation) TPM2_Duplicate (Export, Plain) TPM2_Duplicate (Export, Encrypted) (Symmetric Operation)	RAM:Plaintext Flash:Obfusc ated	N/A	TPM2_ChangeEPS TPM2_ChangePPS TPM2_Startup TPM2_FlushContext TPM2_HierarchyCont rol Clear TPM	Asymmetric Encryption Keys (authValue):Used With Asymmetric Encryption Keys (seedValue):Used With Asymmetric Encryption Keys (sensitive data):Used With Asymmetric Encryption Keys (public data):Used With Symmetric Encryption Keys (authValue):Used With
Asymmetric Encryption Keys (public data)	TPM2_Load TPM2_LoadExternal TPM2_EvictControl TPM2_Create (Import) TPM2_Create (Export) TPM2_CreatePrimary (Import) TPM2_CreatePrimary (Export) TPM2_CreateLoaded TPM2_ReadPublic TPM2_ObjectChangeA uth (Import) TPM2_ObjectChangeA uth (Export) TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation)	RAM:Plaintext Flash:Obfusc ated	N/A	TPM2_ChangeEPS TPM2_ChangePPS TPM2_Startup TPM2_FlushContext TPM2_HierarchyCont rol Clear TPM	Asymmetric Encryption Keys (authValue):Used With Asymmetric Encryption Keys (seedValue):Used With Asymmetric Encryption Keys (sensitive data):Used With Asymmetric Encryption Keys (authPolicy):Used With Symmetric Encryption Keys (authValue):Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	TPM2_Duplicate (Export, Plain) TPM2_Duplicate (Export, Encrypted) (Symmetric Operation)				
Symmetric Encryption Keys (authValue)	TPM2_Load TPM2_LoadExternal TPM2_EvictControl TPM2_Create (Import) TPM2_Create (Export) TPM2_CreatePrimary (Import) TPM2_CreatePrimary (Export) TPM2_CreateLoaded TPM2_ReadPublic TPM2_ObjectChangeAuth (Import) TPM2_ObjectChangeAuth (Export) TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation) TPM2_Duplicate (Export, Plain) TPM2_Duplicate (Export, Encrypted) (Symmetric Operation)	RAM:Plaintext Flash:Obfuscated	N/A	TPM2_ChangeEPS TPM2_ChangePPS TPM2_Startup TPM2_FlushContext TPM2_HierarchyControl Clear TPM	Symmetric Encryption Keys (seedValue):Used With Symmetric Encryption Keys (sensitive data):Used With
Symmetric Encryption Keys (seedValue)	TPM2_Load TPM2_LoadExternal TPM2_EvictControl TPM2_Create (Import) TPM2_Create (Export) TPM2_CreatePrimary (Import) TPM2_CreatePrimary (Export) TPM2_CreateLoaded TPM2_ReadPublic TPM2_ObjectChangeAuth (Import) TPM2_ObjectChangeAuth (Export) TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation) TPM2_Duplicate (Export, Plain) TPM2_Duplicate	RAM:Plaintext Flash:Obfuscated	N/A	TPM2_ChangeEPS TPM2_ChangePPS TPM2_Startup TPM2_FlushContext TPM2_HierarchyControl Clear TPM	Symmetric Encryption Keys (authValue):Used With Symmetric Encryption Keys (sensitive data):Used With ppSeed:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	(Export, Encrypted) (Symmetric Operation)				
Symmetric Encryption Keys (sensitive data)	TPM2_Load TPM2_LoadExternal TPM2_EvictControl TPM2_Create (Import) TPM2_Create (Export) TPM2_CreatePrimary (Import) TPM2_CreatePrimary (Export) TPM2_CreateLoaded TPM2_ReadPublic TPM2_ObjectChangeAuth (Import) TPM2_ObjectChangeAuth (Export) TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation) TPM2_Duplicate (Export, Plain) TPM2_Duplicate (Export, Encrypted) (Symmetric Operation)	RAM:Plaintext Flash:Obfuscated	N/A	TPM2_ChangeEPS TPM2_ChangePPS TPM2_Startup TPM2_FlushContext TPM2_HierarchyControl Clear TPM	Symmetric Encryption Keys (authValue):Used With Symmetric Encryption Keys (seedValue):Used With ppSeed:Derived From
Symmetric Signing Keys (authValue)	TPM2_Load TPM2_LoadExternal TPM2_EvictControl TPM2_Create (Import) TPM2_Create (Export) TPM2_CreatePrimary (Import) TPM2_CreatePrimary (Export) TPM2_CreateLoaded TPM2_ObjectChangeAuth (Import) TPM2_ObjectChangeAuth (Export) TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation)	RAM:Plaintext Flash:Obfuscated	N/A	TPM2_ChangeEPS TPM2_ChangePPS TPM2_Startup TPM2_FlushContext TPM2_HierarchyControl Clear TPM	Symmetric Signing Keys (seedValue):Used With Symmetric Signing Keys (sensitive data):Used With
Symmetric Signing Keys (seedValue)	TPM2_Load TPM2_LoadExternal TPM2_EvictControl TPM2_Create (Import) TPM2_Create (Export) TPM2_CreatePrimary (Import)	RAM:Plaintext Flash:Obfuscated	N/A	TPM2_ChangeEPS TPM2_ChangePPS TPM2_Startup TPM2_FlushContext TPM2_HierarchyControl Clear TPM	Symmetric Signing Keys (authValue):Used With Symmetric Signing Keys (sensitive data):Used With ppSeed:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	TPM2_CreatePrimary (Export) TPM2_CreateLoaded TPM2_ObjectChangeAuth (Import) TPM2_ObjectChangeAuth (Export) TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation)				
Symmetric Signing Keys (sensitive data)	TPM2_Load TPM2_LoadExternal TPM2_EvictControl TPM2_Create (Import) TPM2_Create (Export) TPM2_CreatePrimary (Import) TPM2_CreatePrimary (Export) TPM2_CreateLoaded TPM2_ObjectChangeAuth (Import) TPM2_ObjectChangeAuth (Export) TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation)	RAM:Plaintext Flash:Obfuscated	N/A	TPM2_ChangeEPS TPM2_ChangePPS TPM2_Startup TPM2_FlushContext TPM2_HierarchyControl Clear TPM	Symmetric Signing Keys (authValue):Used With Symmetric Signing Keys (seedValue):Used With ppSeed:Derived From
Object Ephemeral Keys (symKey)	TPM2_Load TPM2_Create (Import) TPM2_Create (Export) TPM2_CreateLoaded TPM2_ObjectChangeAuth (Import) TPM2_ObjectChangeAuth (Export)	Stack:Plaintext	Until no longer needed, or power reset.	Stack Cleaning	Object Ephemeral Keys (hmacKey):Used With Asymmetric Signing Keys (authValue):Encrypts Asymmetric Signing Keys (seedValue):Encrypts Asymmetric Signing Keys (sensitive data):Encrypts Asymmetric Signing Keys (authPolicy):Encrypts Asymmetric Signing Keys (public data):Encrypts Asymmetric Encryption Keys (authValue):Encrypts Asymmetric Encryption Keys (seedValue):Encrypts Asymmetric Encryption

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Keys (sensitive data):Encrypts Asymmetric Encryption Keys (authPolicy):Encrypts Asymmetric Encryption Keys (public data):Encrypts Symmetric Encryption Keys (authValue):Encrypts Symmetric Encryption Keys (seedValue):Encrypts Symmetric Encryption Keys (sensitive data):Encrypts Symmetric Signing Keys (authValue):Encrypts Symmetric Signing Keys (seedValue):Encrypts Symmetric Signing Keys (sensitive data):Encrypts Asymmetric Signing Keys (authValue):Decrypts Asymmetric Signing Keys (seedValue):Decrypts Asymmetric Signing Keys (sensitive data):Decrypts Asymmetric Signing Keys (authPolicy):Decrypts Asymmetric Signing Keys (public data):Decrypts Asymmetric Encryption Keys (authValue):Decrypts Asymmetric Encryption Keys (seedValue):Decrypts Asymmetric Encryption Keys (sensitive data):Decrypts Asymmetric Encryption Keys (authPolicy):Decrypts Asymmetric Encryption Keys (public

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					data):Decrypts Symmetric Encryption Keys (authValue):Decrypts Symmetric Encryption Keys (seedValue):Decrypts Symmetric Encryption Keys (sensitive data):Decrypts Symmetric Signing Keys (authValue):Decrypts Symmetric Signing Keys (seedValue):Decrypts Symmetric Signing Keys (sensitive data):Decrypts Asymmetric Signing Keys (seedValue):Derived From Asymmetric Encryption Keys (seedValue):Derived From Symmetric Encryption Keys (seedValue):Derived From Symmetric Signing Keys (seedValue):Derived From
Object Ephemeral Keys (hmacKey)	TPM2_Load TPM2_LoadExternal TPM2_Create (Import) TPM2_Create (Export) TPM2_CreateLoaded TPM2_ObjectChangeAuth (Import) TPM2_ObjectChangeAuth (Export)	Stack:Plaintext	Until no longer needed, or power reset.	Stack Cleaning	Object Ephemeral Keys (symKey):Used With Asymmetric Signing Keys (seedValue):Derived From Asymmetric Encryption Keys (seedValue):Derived From Symmetric Encryption Keys (seedValue):Derived From Symmetric Signing Keys (seedValue):Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Duplication Ephemeral Keys (symKey)	TPM2_Import TPM2_Rewrap (Import) (Asymmetric Operation) TPM2_Rewrap (Export) (Asymmetric Operation) TPM2_Duplicate (Import, Plain) TPM2_Duplicate (Import, Encrypted) (Asymmetric Operation) TPM2_Duplicate (Export, Encrypted) (Asymmetric Operation)	Stack:Plaintext	Until no longer needed, or power reset.	Stack Cleaning	Duplication Ephemeral Keys (hmacKey):Used With Duplication Ephemeral Keys (innerSymKey):Used With Asymmetric Signing Keys (authValue):Encrypts Asymmetric Signing Keys (seedValue):Encrypts Asymmetric Signing Keys (sensitive data):Encrypts Asymmetric Signing Keys (authPolicy):Encrypts Asymmetric Signing Keys (public data):Encrypts Asymmetric Encryption Keys (authValue):Encrypts Asymmetric Encryption Keys (seedValue):Encrypts Asymmetric Encryption Keys (sensitive data):Encrypts Asymmetric Encryption Keys (authPolicy):Encrypts Asymmetric Encryption Keys (public data):Encrypts Symmetric Encryption Keys (authValue):Encrypts Symmetric Encryption Keys (seedValue):Encrypts Symmetric Encryption Keys (sensitive data):Encrypts Symmetric Signing Keys (authValue):Encrypts Symmetric Signing Keys (seedValue):Encrypts Symmetric Signing Keys (sensitive

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					data):Encrypts Asymmetric Signing Keys (authValue):Decrypts Asymmetric Signing Keys (seedValue):Decrypts Asymmetric Signing Keys (sensitive data):Decrypts Asymmetric Signing Keys (authPolicy):Decrypts Asymmetric Signing Keys (public data):Decrypts Asymmetric Encryption Keys (authValue):Decrypts Asymmetric Encryption Keys (seedValue):Decrypts Asymmetric Encryption Keys (sensitive data):Decrypts Asymmetric Encryption Keys (authPolicy):Decrypts Asymmetric Encryption Keys (public data):Decrypts Symmetric Encryption Keys (authValue):Decrypts Symmetric Encryption Keys (seedValue):Decrypts Symmetric Encryption Keys (sensitive data):Decrypts Symmetric Signing Keys (authValue):Decrypts Symmetric Signing Keys (seedValue):Decrypts Symmetric Signing Keys (sensitive data):Decrypts Ephemeral Key Agreement Keys:Derived From DRBG state:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Duplication Ephemeral Keys (hmacKey)	TPM2_Import TPM2_Rewrap (Import) (Asymmetric Operation) TPM2_Rewrap (Export) (Asymmetric Operation) TPM2_Duplicate (Import, Plain) TPM2_Duplicate (Import, Encrypted) (Asymmetric Operation) TPM2_Duplicate (Export, Encrypted) (Asymmetric Operation)	Stack:Plaintext	Until no longer needed, or power reset.	Stack Cleaning	Duplication Ephemeral Keys (symKey):Used With Duplication Ephemeral Keys (innerSymKey):Used With Ephemeral Key Agreement Keys:Derived From DRBG state:Derived From
Duplication Ephemeral Keys (innerSymKey)	TPM2_Rewrap (Import) (Symmetric Operation) TPM2_Rewrap (Export) (Symmetric Operation) TPM2_Import TPM2_Duplicate (Import, Plain) TPM2_Duplicate (Import, Encrypted) (Symmetric Operation)	Stack:Plaintext	Until no longer needed, or power reset.	Stack Cleaning	Duplication Ephemeral Keys (symKey):Used With Duplication Ephemeral Keys (hmacKey):Used With Asymmetric Signing Keys (authValue):Encrypts Asymmetric Signing Keys (seedValue):Encrypts Asymmetric Signing Keys (sensitive data):Encrypts Asymmetric Signing Keys (authPolicy):Encrypts Asymmetric Signing Keys (public data):Encrypts Asymmetric Encryption Keys (authValue):Encrypts Asymmetric Encryption Keys (seedValue):Encrypts Asymmetric Encryption Keys (sensitive data):Encrypts Asymmetric Encryption Keys (authPolicy):Encrypts Asymmetric Encryption Keys (public data):Encrypts Symmetric Encryption Keys (authValue):Encrypts Symmetric Encryption

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Keys (seedValue):Encrypts Symmetric Encryption Keys (sensitive data):Encrypts Symmetric Signing Keys (authValue):Encrypts Symmetric Signing Keys (seedValue):Encrypts Symmetric Signing Keys (sensitive data):Encrypts Asymmetric Signing Keys (authValue):Decrypts Asymmetric Signing Keys (seedValue):Decrypts Asymmetric Signing Keys (sensitive data):Decrypts Asymmetric Signing Keys (authPolicy):Decrypts Asymmetric Signing Keys (public data):Decrypts Asymmetric Encryption Keys (authValue):Decrypts Asymmetric Encryption Keys (seedValue):Decrypts Asymmetric Encryption Keys (sensitive data):Decrypts Asymmetric Encryption Keys (authPolicy):Decrypts Asymmetric Encryption Keys (public data):Decrypts Symmetric Encryption Keys (authValue):Decrypts Symmetric Encryption Keys (seedValue):Decrypts Symmetric Encryption Keys (sensitive data):Decrypts Symmetric Signing Keys

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					(authValue):Decrypts Symmetric Signing Keys (seedValue):Decrypts Symmetric Signing Keys (sensitive data):Decrypts
Context Ephemeral Keys (symKey)	TPM2_ContextLoad TPM2_ContextSave	Stack:Plaintext	Until no longer needed, or power reset.	Stack Cleaning	Context Ephemeral Keys (hmacKey):Used With Session (salt):Encrypts Session (salt):Decrypts phProof:Derived From
Context Ephemeral Keys (hmacKey)	TPM2_ContextLoad TPM2_ContextSave	Stack:Plaintext	Until no longer needed, or power reset.	Stack Cleaning	Context Ephemeral Keys (symKey):Used With phProof:Derived From
Credential Ephemeral Keys (symKey)	TPM2_MakeCredential TPM2_ActivateCredential	Stack:Plaintext	Until no longer needed, or power reset.	Stack Cleaning	Credential Ephemeral Keys (hmacKey):Used With Asymmetric Signing Keys (authValue):Encrypts Asymmetric Signing Keys (seedValue):Encrypts Asymmetric Signing Keys (sensitive data):Encrypts Asymmetric Signing Keys (authPolicy):Encrypts Asymmetric Signing Keys (public data):Encrypts Asymmetric Encryption Keys (authValue):Encrypts Asymmetric Encryption Keys (seedValue):Encrypts Asymmetric Encryption Keys (sensitive data):Encrypts Asymmetric Encryption Keys (authPolicy):Encrypts

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Asymmetric Encryption Keys (public data):Encrypts Symmetric Encryption Keys (authValue):Encrypts Symmetric Encryption Keys (seedValue):Encrypts Symmetric Encryption Keys (sensitive data):Encrypts Symmetric Signing Keys (authValue):Encrypts Symmetric Signing Keys (seedValue):Encrypts Symmetric Signing Keys (sensitive data):Encrypts Asymmetric Signing Keys (authValue):Decrypts Asymmetric Signing Keys (seedValue):Decrypts Asymmetric Signing Keys (sensitive data):Decrypts Asymmetric Signing Keys (authPolicy):Decrypts Asymmetric Signing Keys (public data):Decrypts Asymmetric Encryption Keys (authValue):Decrypts Asymmetric Encryption Keys (seedValue):Decrypts Asymmetric Encryption Keys (sensitive data):Decrypts Asymmetric Encryption Keys (authPolicy):Decrypts Asymmetric Encryption Keys (public data):Decrypts Symmetric Encryption Keys (authValue):Decrypts Symmetric Encryption

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Keys (seedValue):Decrypts Symmetric Encryption Keys (sensitive data):Decrypts Symmetric Signing Keys (authValue):Decrypts Symmetric Signing Keys (seedValue):Decrypts Symmetric Signing Keys (sensitive data):Decrypts Ephemeral Key Agreement Keys:Derived From Asymmetric Encryption Keys (sensitive data):Derived From DRBG state:Derived From
Credential Ephemeral Keys (hmacKey)	TPM2_MakeCredential TPM2_ActivateCredential	Stack:Plaintext	Until no longer needed, or power reset.	Stack Cleaning	Credential Ephemeral Keys (symKey):Used With Ephemeral Key Agreement Keys:Derived From Asymmetric Encryption Keys (sensitive data):Derived From DRBG state:Derived From
Ephemeral Key Agreement Keys		Stack:Plaintext	Until no longer needed, or power reset.	Stack Cleaning	
Ephemeral User ECC Keys	TPM2_Load TPM2_LoadExternal	Stack:Plaintext	Until no longer needed, or power reset.	Stack Cleaning	
Endorsement Keys (private values)	TPM2_CreatePrimary (Import)	Flash:Obfuscated	N/A	TPM2_ChangeEPS Clear TPM	Endorsement Keys (public values):Paired

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					With epSeed:Used With
Endorsement Keys (public values)		Flash:Obfuscated	N/A	TPM2_ChangeEPS Clear TPM	Endorsement Keys (private values):Paired With epSeed:Used With
Firmware Update Keys (ECC)		Flash:Obfuscated	N/A	Clear TPM	Firmware Update Keys (AES):Used With
Firmware Update Keys (AES)		Flash:Obfuscated	N/A	Clear TPM	Firmware Update Keys (ECC):Used With
NV Index (authValue)	TPM2_NV_ChangeAuth (Import) TPM2_NV_ChangeAuth (Export)	Flash:Obfuscated	N/A	TPM2_Clear TPM2_ChangeEPS TPM2_ChangePPS TPM2_NV_Undefine Space Clear TPM	NV Index (authPolicy):Used With
NV Index (authPolicy)	TPM2_NV_ChangeAuth (Import) TPM2_NV_ChangeAuth (Export)	Flash:Obfuscated	N/A	TPM2_Clear TPM2_ChangeEPS TPM2_ChangePPS TPM2_NV_Undefine Space Clear TPM	NV Index (authValue):Used With
Session (salt)	TPM2_ContextLoad TPM2_ContextSave	Stack:Plaintext	N/A	Stack Cleaning	
Session (sessionKey)		RAM:Plaintext	N/A	TPM2_Startup TPM2_FlushContext	phProof:Used With ehProof:Used With shProof:Used With nullProof:Used With Session (salt):Derived From
Session (symKey)		Stack:Plaintext	N/A	Stack Cleaning	Session (sessionKey):Derived From
DRBG state		RAM:Plaintext Flash:Obfuscated	N/A	TPM2_Startup Clear TPM	DRBG Entropy Input:Derived From
DRBG Entropy Input		RAM:Plaintext Flash:Obfuscated	N/A	TPM2_Startup Clear TPM	DRBG state:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Transient DRBG state		RAM:Plaintext Flash:Obfuscated	N/A	TPM2_Startup Clear TPM	DRBG Entropy Input:Derived From
finished_key				SPDM session reset	rspHandshakeSecret:Derived From
SPDM ECDH Shared Secret				SPDM session reset	
reqHandshakeSecret				SPDM session reset	SPDM ECDH Shared Secret:Derived From PSK:Derived From
rspHandshakeSecret				SPDM session reset	SPDM ECDH Shared Secret:Derived From PSK:Derived From
ReqEncKey				SPDM session reset	SPDM ECDH Shared Secret:Derived From PSK:Derived From
RspEncKey				SPDM session reset	SPDM ECDH Shared Secret:Derived From PSK:Derived From
PSK				PSK Clear	
requester identity signature verification public key				SPDM session reset	
requester identity signature verification private key					
TPM ECDH Shared Secret					Ephemeral User ECC Keys:Established by Asymmetric Encryption Keys (sensitive data):Established by Asymmetric Encryption Keys (public data):Established by
responder identity signature verification public key	SPDM Session Establish				

Table 21: SSP Table 2

## 9.5 Transitions

SHA-1 is disallowed for digital signature generation. When used for digital signature verification, SHA-1 is allowed for legacy use. The use of SHA-1 is deprecated through December 31, 2030, for applying protection in non-digital signature applications and disallowed thereafter. The use of SHA-1 is acceptable for processing already-protected information through December 31, 2030, and allowed for legacy use thereafter.

## 10 Self-Tests

### 10.1 Pre-Operational Self-Tests

The Module implements the following tests during power-on:

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A6386)	HMAC-SHA2-256	Message Authentication Code (MAC)	SW/FW Integrity	Successful boot	Performed on system startup

Table 22: Pre-Operational Self-Tests

The module does not provide any cryptographic services prior to this test.

### 10.2 Conditional Self-Tests

The Module implements the following conditional tests:

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Counter DRBG (A6386)	256-bit key	KAT	CAST	Successful boot	SP 800-90Ar1 section 11.3 (instantiate, reseed, generate) health test	Upon or before first invocation of service that uses the algorithm.
HMAC-SHA2-384 (A6386)	384 bit keys	KAT	CAST	Successful boot	Verify	Upon or before first invocation of service that uses the algorithm.
KDF SP800-108 (A6386)	SHA2-256	KAT	CAST	Successful boot	Key Derivation	Upon or before first invocation of service that uses the algorithm.
KDA OneStep Sp800-56Cr1 (A6386)	SHA2-256	KAT	CAST	Successful boot	Key Derivation	Upon or before first invocation of service that uses the algorithm.
SHA-1 (A6386)	SHA-1	KAT	CAST	Successful boot	Message Digest	Upon or before first invocation of service that

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						uses the algorithm.
SHA2-256 (A6386)	SHA2-256	KAT	CAST	Successful boot	Message Digest	Upon or before first invocation of service that uses the algorithm.
SHA2-384 (A6386)	SHA2-384	KAT	CAST	Successful boot	Message Digest	Upon or before first invocation of service that uses the algorithm.
AES-CFB128 (A6386)	128, 256 bit keys	KAT	CAST	Successful boot	Encryption	Upon or before first invocation of service that uses the algorithm.
AES-CFB128 (A6386)	128, 256 bit keys	KAT	CAST	Successful boot	Decryption	Upon or before first invocation of service that uses the algorithm.
AES-CTR (A6386)	128, 256 bit keys	KAT	CAST	Successful boot	Encryption	Upon or before first invocation of service that uses the algorithm.
AES-CTR (A6386)	128, 256 bit keys	KAT	CAST	Successful boot	Decryption	Upon or before first invocation of service that uses the algorithm.
AES-OFB (A6386)	128, 256 bit keys	KAT	CAST	Successful boot	Encryption	Upon or before first invocation of service that uses the algorithm.
AES-OFB (A6386)	128, 256 bit keys	KAT	CAST	Successful boot	Decryption	Upon or before first invocation of

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						service that uses the algorithm.
AES-GCM (A6386)	256-bit key	KAT	CAST	Successful boot	Authenticated Encryption	Upon or before first invocation of service that uses the algorithm.
AES-GCM (A6386)	256-bit key	KAT	CAST	Successful boot	Authenticated Decryption	Upon or before first invocation of service that uses the algorithm.
RSA SigGen (FIPS186-5) (A6386)	2048-bit modulus; Hash: SHA2-256	KAT	CAST	Successful boot	Signature Generation	Upon or before first invocation of service that uses the algorithm.
RSA SigVer (FIPS186-5) (A6386)	2048-bit modulus; Hash: SHA2-256	KAT	CAST	Successful boot	Signature Verification	Upon or before first invocation of service that uses the algorithm.
ECDSA SigGen (FIPS186-5) (A6386)	Curve: P-256; Hash: SHA2-256	KAT	CAST	Successful boot	Signature Generation	Upon or before first invocation of service that uses the algorithm.
ECDSA SigVer (FIPS186-5) (A6386)	Curve: P-256; Hash: SHA2-256	KAT	CAST	Successful boot	Signature Verification	Upon or before first invocation of service that uses the algorithm.
KAS-ECC-SSC Sp800-56Ar3 (A6386)	Curve: P-256	KAT	CAST	Successful boot	Shared Secret Computation	Upon or before first invocation of service that uses the algorithm.
KTS-IFC (A6386)	2048-bit modulus	KAT	CAST	Successful boot	RSA Key Transport (Encapsulation/Decapsulation)	Upon or before first

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						invocation of service that uses the algorithm.
ECDsa KeyGen (FIPS186-5) (A6386)	P-256, P-384 curves	PCT	PCT	Key pair returned to caller	Signature Generation / Signature Verification	Performed every time ECC key pair is generated
RSA KeyGen (FIPS186-5) (A6386)	2048, 3072, 4096 bit keys	PCT	PCT	Key pair returned to caller	Encryption / Decryption tested for RSA key pairs generated for approved key transport and Signature Generation / Signature Verification tested for RSA key pairs generated for digital signatures	Performed every time RSA key pair is generated
KDA HKDF Sp800-56Cr1 (A6386)	HMAC-SHA2-384	KAT	CAST	Successful boot	Key Derivation	Upon or before first invocation of service that uses the algorithm.
HMAC-SHA2-256 (A6386)	256 bit keys	KAT	CAST	Successful boot	Verify	Upon or before first invocation of service that uses the algorithm.
ESV - Repetition Count Test (Startup)	Startup test with 1024 samples; Cutoff value = 39	fault-detection test	CAST	successful seeding of SP 800-90A DRBG	SP 800-90B 4.4.1 Repetition Count Test	upon seeding or reseeding SP 800-90A DRBG
ESV - Adaptive Proportional Test (Startup)	Startup test with 1024 samples; Cutoff value = 793	fault-detection test	CAST	successful seeding of SP 800-90A DRBG	SP 800-90B 4.4.2 Adaptive Proportion Test	upon seeding or reseeding SP 800-90A DRBG
ESV - Repetition Count Test (Continuous)	Cutoff value = 39	fault-detection test	CAST	successful seeding of SP 800-90A DRBG	SP 800-90B 4.4.1 Repetition Count Test	upon seeding or reseeding SP 800-90A DRBG
ESV - Adaptive Proportional Test (Continuous)	Cutoff value = 793	fault-detection test	CAST	successful seeding of SP 800-90A DRBG	SP 800-90B 4.4.2 Adaptive Proportion Test	upon seeding or reseeding SP 800-90A DRBG

Table 23: Conditional Self-Tests

No services are available, and input and output are inhibited while performing the self-test.

### 10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A6386)	Message Authentication Code (MAC)	SW/FW Integrity	On demand	Manually

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG (A6386)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A6386)	KAT	CAST	On demand	Manually
KDF SP800-108 (A6386)	KAT	CAST	On demand	Manually
KDA OneStep Sp800-56Cr1 (A6386)	KAT	CAST	On demand	Manually
SHA-1 (A6386)	KAT	CAST	On demand	Manually
SHA2-256 (A6386)	KAT	CAST	On demand	Manually
SHA2-384 (A6386)	KAT	CAST	On demand	Manually
AES-CFB128 (A6386)	KAT	CAST	On demand	Manually
AES-CFB128 (A6386)	KAT	CAST	On demand	Manually
AES-CTR (A6386)	KAT	CAST	On demand	Manually
AES-CTR (A6386)	KAT	CAST	On demand	Manually
AES-OFB (A6386)	KAT	CAST	On demand	Manually
AES-OFB (A6386)	KAT	CAST	On demand	Manually
AES-GCM (A6386)	KAT	CAST	On demand	Manually
AES-GCM (A6386)	KAT	CAST	On demand	Manually
RSA SigGen (FIPS186-5) (A6386)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A6386)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigGen (FIPS186-5) (A6386)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A6386)	KAT	CAST	On demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A6386)	KAT	CAST	On demand	Manually
KTS-IFC (A6386)	KAT	CAST	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A6386)	PCT	PCT	N/A	N/A
RSA KeyGen (FIPS186-5) (A6386)	PCT	PCT	N/A	N/A
KDA HKDF Sp800-56Cr1 (A6386)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A6386)	KAT	CAST	On demand	Manually
ESV - Repetition Count Test (Startup)	fault-detection test	CAST	On demand	Manually
ESV - Adaptive Proportional Test (Startup)	fault-detection test	CAST	On demand	Manually
ESV - Repetition Count Test (Continuous)	fault-detection test	CAST	On demand	Manually
ESV - Adaptive Proportional Test (Continuous)	fault-detection test	CAST	On demand	Manually

Table 25: Conditional Periodic Information

### 10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
General Failure	General Failure	Endorsement Key creation failure, Internal NV inconsistency Fingerprint value in TPM2_ContextLoad doesn't match Post-field upgrade problem	Platform Reset or power cycle	returns TPM_RC_FAILURE

Name	Description	Conditions	Recovery Method	Indicator
Self-Test Failure	Failure in conditional CAST, Conditional PCT or FW Integrity Test failure	Internal integrity error - indicative of fault injection attack or internal functional fault	Power cycle	returns SELF_TEST_FAILURE
SP 800-90B Health Tests Failure	Failure in RCT or APT SP 800-90B health tests	random number generation failure	Power cycle	returns ERR_RNG_RANDOM_FAIL

Table 26: Error States

If a conditional or power-on self-test fails, the Module enters an error state where both data output and cryptographic services are disabled. The Module can recover from this error state once all self-tests pass after a platform reset or power cycle.

## 10.5 Operator Initiation of Self-Tests

The module allows operators to initiate the pre-operational or conditional cryptographic algorithm self-tests on demand for periodic testing, by power-cycling the module.

## 11 Life-Cycle Assurance

### 11.1 Installation, Initialization, and Startup Procedures

To install the module in the FIPS validated environment of operation, do the following:

- The module must be controlled physically during the installation.
- The module must be connected on the PCB as described in the Module technical specifications. The connection must ensure one-to-one binding with the platform.
- The platform on which the module is installed should include BIOS and OS that initialize and control TPM hierarchies and set hierarchy's authorization value and policy. If the platform does not have such BIOS and OS, the crypto-officer shall install software to manage TPM hierarchies and set the hierarchy's authorization and policy.

### 11.2 Administrator Guidance

The module's firmware may only be upgraded by a Crypto Officer calling NTC\_FIELD\_UPGRADE service. The module will perform a firmware load test, and if successful will perform a firmware upgrade. Any firmware loaded into this module that is not shown on the module certificate is out of the scope of this validation and requires a separate FIPS 140-3 validation. Running any firmware version not listed on the modules validation list, will result in running a non-validated module

### 11.3 Non-Administrator Guidance

The security policy provides all the details about how the module meets FIPS compliance. For, further details on TCG's Trusted Platform Module specification, refer to the TCG guidance TPM2.0 Revision 1.59.

## 12 Mitigation of Other Attacks

The module does not claim any mitigation of other attacks.

## References

FIPS140-3	FIPS PUB 140-3 - Security Requirements for Cryptographic Modules March 2019 <a href="https://doi.org/10.6028/NIST.FIPS.140-3">https://doi.org/10.6028/NIST.FIPS.140-3</a>
FIPS140-3_IG	Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program December 20, 2024 <a href="https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips_140-3/FIPS_140-3_IG.pdf">https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips_140-3/FIPS_140-3_IG.pdf</a>
TCG TPM v2.0 Provisioning Guidance Version 1.0 Revision 1.0	TCG TPM v2.0 Provisioning Guidance Version 1.0 Revision 1.0 March 15, 2017 <a href="https://trustedcomputinggroup.org/tcg-tpm-v2-0-provisioning-guidance">https://trustedcomputinggroup.org/tcg-tpm-v2-0-provisioning-guidance</a>
TPM Library Specification Errata	Errata for TCG Trusted Platform Module Library Family "2.0" Level 00 Revision 01.59 Version 1.7 June 10, 2025 <a href="https://trustedcomputinggroup.org/wp-content/uploads/Errata-Version-1.7-for-Trusted-Platform-Module-Library-Specification-Family-2.0-Revision-01.59_Pub.pdf">https://trustedcomputinggroup.org/wp-content/uploads/Errata-Version-1.7-for-Trusted-Platform-Module-Library-Specification-Family-2.0-Revision-01.59_Pub.pdf</a>
Platform TPM Profile Specification	TCG PC Client Platform TPM Profile Specification for TPM 2.0 September 4, 2020 <a href="https://trustedcomputinggroup.org/wp-content/uploads/PC-Client-Specific-Platform-TPM-Profile-for-TPM-2p0-v1p05p_r14_pub.pdf">https://trustedcomputinggroup.org/wp-content/uploads/PC-Client-Specific-Platform-TPM-Profile-for-TPM-2p0-v1p05p_r14_pub.pdf</a>
SPDM 1.3.2	Security Protocol and Data Model (SPDM) Specification, version 1.3.2 <a href="https://www.dmtf.org/sites/default/files/standards/documents/DSP0274_1.3.2.pdf">https://www.dmtf.org/sites/default/files/standards/documents/DSP0274_1.3.2.pdf</a>
FIPS180-4	Secure Hash Standard (SHS) March 2012 <a href="https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf">https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf</a>
FIPS 186-4	Digital Signature Standard (DSS) July 2013 <a href="https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf">https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf</a>
FIPS 186-5	Digital Signature Standard (DSS) February 2023 <a href="https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf">https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf</a>
FIPS197	Advanced Encryption Standard November 2001 <a href="https://csrc.nist.gov/publications/fips/fips197/fips-197.pdf">https://csrc.nist.gov/publications/fips/fips197/fips-197.pdf</a>
FIPS198-1	The Keyed Hash Message Authentication Code (HMAC) July 2008 <a href="https://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf">https://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf</a>
PKCS#1	Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 February 2003 <a href="https://www.ietf.org/rfc/rfc3447.txt">https://www.ietf.org/rfc/rfc3447.txt</a>

SP800-38Arev1	NIST Special Publication 800-38A - Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001 <a href="https://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf">https://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf</a>
SP800-38B	NIST Special Publication 800-38B - Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication May 2005 <a href="https://csrc.nist.gov/publications/detail/sp/800-38b/final">https://csrc.nist.gov/publications/detail/sp/800-38b/final</a>
SP800-38C	NIST Special Publication 800-38C - Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality May 2004 <a href="https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf">https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf</a>
SP800-38D	NIST Special Publication 800-38D - Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC November 2007 <a href="https://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf">https://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf</a>
SP800-56Arev3	NIST Special Publication 800-56A Revision 2 - Recommendation for Pair Wise Key Establishment Schemes Using Discrete Logarithm Cryptography April 2018 <a href="https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf">https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf</a>
SP800-57rev5	NIST Special Publication 800-57 Part 1 Revision 5 - Recommendation for Key Management Part 1: General May 2020 <a href="https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf">https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf</a>
SP800-90Arev1	NIST Special Publication 800-90A - Revision 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators June 2015 <a href="https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf">https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf</a>
SP800-90B	NIST Special Publication 800-90B - Recommendation for the Entropy Sources Used for Random Bit Generation January 2018 <a href="https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf">https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf</a>
SP800-131Arev2	NIST Special Publication 800-131A Revision 2 - Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths March 2019 <a href="https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf">https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf</a>
SP800-133rev2	NIST Special Publication 800-133 Revision 2 - Recommendation for Cryptographic Key Generation June 2020 <a href="https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf">https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf</a>
SP800-135rev1	NIST Special Publication 800-135 Revision 1 - Recommendation for Existing Application-Specific Key Derivation Functions December 2011 <a href="https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf">https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf</a>

SP800-140Br1

NIST Special Publication 800-140Br1 - CMVP Security Policy Requirements  
November 2023

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140Br1.pdf>