NPCT7xx TPM 2.0 rev 1.59
FIPS 140-2 Security Policy

Revision 1.0.7

Revision Record

Revision	Date	Comments
0.8.0	May 25, 2021	Preliminary version
0.9.0	May 30, 2021	Updated Table 4 according to convention
1.0.0	June 1, 2021	Changes following review
1.0.1	June 3, 2021	Changes following review
1.0.2	September 23, 2021	Streamlined Tables 4 and 5
1.0.3	October 5, 2021	Updated CAVP Certificate in Table 4
1.0.4	October 6, 2021	Removed redundant text from Sections 2.1 and 2.2
1.0.5	December 1, 2021	Changed ENT to ENT (P) in Table 4
1.0.6	January 19, 2022	Added Firmware version 7.2.3.1
1.0.7	January 11, 2023	Added “Operational Environment” section (1.3). Added reference [3] to “References” section (13). Refined the explanation and added references to [3] in “Authentication” section (4.1). In Table 4: - Changed RSADP entry to CVL. - Changed KTS-AES entry to KTS (global change) and updated the Use column. - In KTS-RSA entry, removed one mode and updated the Use column. - Changed the reference from SP800-56B to SP800-56Br2. - Added DRBG Conditioning Component. - In ENT (P) entry, removed footnote. Added “Key Generation and Entropy” section (5.1). Changed the title of section 2.2 to “Non-Approved, Not Allowed Algorithms” and added a new footnote in Table 5. In Table 8 updated Firmware Update entry and added a footnote. In Table 9, changed “NDRBG” and “NDRNG” to “ENT (P)”. In Table 10, added ENT (P) (Health Test) and changed KDFe to KDA. In Acronym section (12) “SP” changed to “SP800” (NIST Special Publication). Added guidance to “Object Import” section (9.5).

Table of Contents

Figures

Tables

1. Module Description

1.1 General Description

The Nuvoton Trusted Platform Module (“Module”) is a hardware cryptographic module that implements advanced cryptographic algorithms, including symmetric and asymmetric cryptography, as well as key generation and random number generation.

The Module is a single-chip module that provides cryptographic services utilized by external applications. The Module meets the requirements of FIPS Pub 140-2.

The Module meets commercial-grade specifications for power, temperature, reliability, shock, and vibrations, and includes chip packaging to meet the physical security requirements at Physical Security Level 3. In addition, it meets EMI/EMC Security Level 3.

The FIPS 140-2 conformance testing was performed on the following configurations of the Nuvoton NPCT7xx TPM 2.0:

- Firmware version: 7.2.3.0, 7.2.3.1
- Hardware version 1: LAG019 in TSSOP28 package
- Hardware version 2: LAG019 in QFN32 package
- Hardware version 3: LAG019 in UQFN16 package

The TPM2.0 packages are shown below.

Figure 1. LAG019 in QFN32 Package

Figure 2. LAG019 in UQFN16 Package

Figure 3. LAG019 in TSSOP28 Package

The physical cryptographic boundary of the Module is the outer boundary of the chip packaging.

Figure 4 shows a logical diagram of the Module:

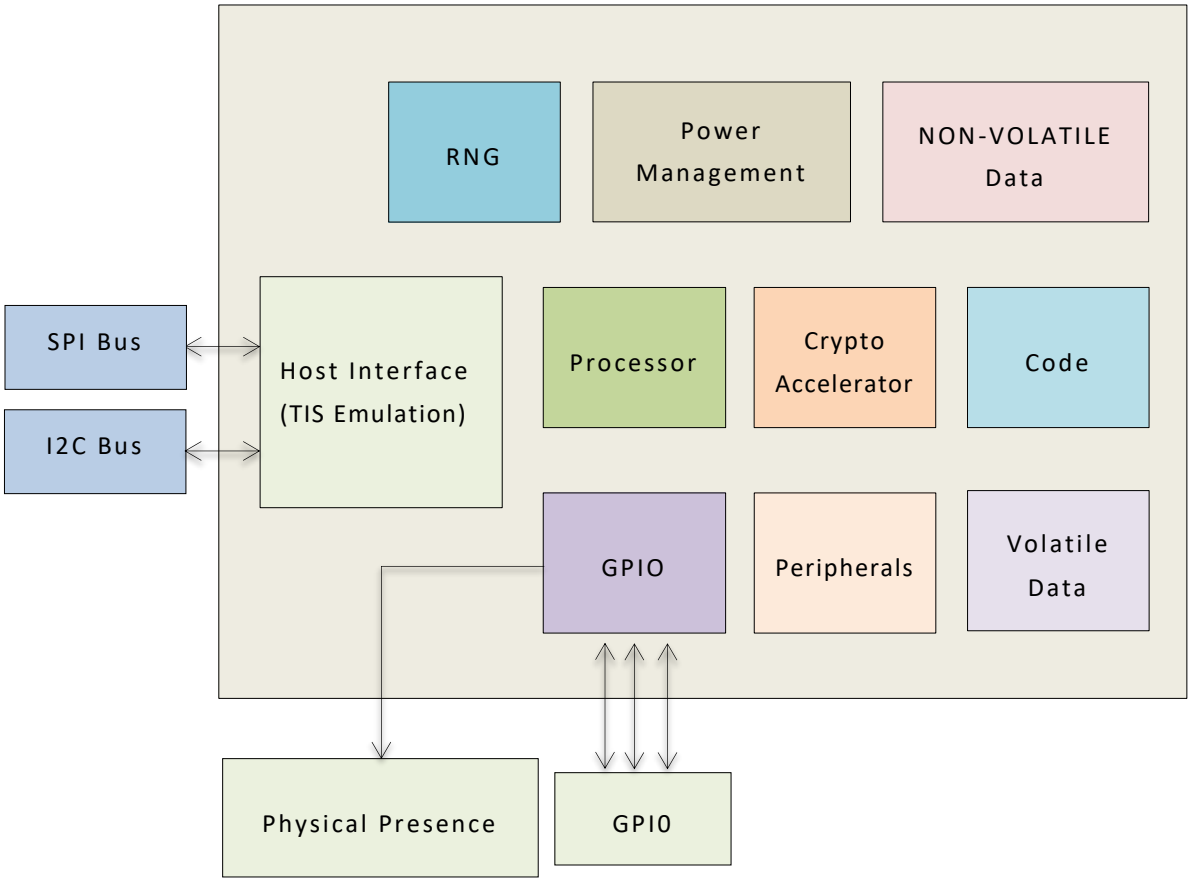

Figure 4. TPM 2.0 Logical Block Diagram

The Module was tested to meet overall Security Level 2 of the FIPS PUB 140-2 standard. The Security Level for each section of FIPS PUB 140-2 is specified in Table 1.

Table 1. Security Levels

FIPS 140-2 Section	Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

1.2 Approved Modes

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.

1.2.1 Approved Mode 1

This mode is the default mode when the TPM powers up.

Table 2. Approved Mode 1

Properties	Description
Definition	Transient mode
Configuration	This mode is the default when the TPM powers up. It assumes a list of basic algorithms (listed in 'Algorithms used' row) that are going to be used for basic TPM commands. These algorithms are tested in _TPM_Init, i.e., before the first command is executed.
Services available	All services that do not use asymmetric cryptography (RSA, ECDSA, ECDH)
Algorithms used	SHS (SHA-1, SHA2-256, SHA2-384) / HMAC / AES / DRBG / KBKDF / KDFe
CSPs used	Only asymmetric CSPs (RSA and ECC keys) cannot be used
Self tests	SHS (SHA-1, SHA2-256, SHA2-384) / HMAC / AES / DRBG / KBKDF / KDFe and firmware integrity test

1.2.2 Approved Mode 2

This mode is the Approved mode of operation when all CSPs are accessible.

Table 3. Approved Mode 2

Properties	Description
Definition	Full Approved mode of operation
Configuration	There are three ways to move to Mode 2: 1. TPM2_SelfTest(fullTest = YES) command. 2. TPM2_SelfTest(fullTest = NO) command. If the firmware is in Mode 1, the command returns TPM_RC_TESTING. Immediately after that, the firmware runs a self test equivalent to TPM2_SelfTest(fullTest = YES). If a command is received before the TPM has completed self test execution, the TPM will first complete SelfTest and then execute the command. 3. Command that requires Mode 2 (all commands not listed in PTP section 5.5.1.6, Self Test and Early Platform Initialization). Incremental ST does not move to Mode 2 even if all the algorithm testing is completed using this command.
Services available	All services
Algorithms used	All supported algorithms
CSPs used	All CSPs
Self tests	SHS (SHA-1, SHA2-256, SHA2-384) / HMAC / AES / DRBG / KBKDF / KDFe / RSA / ECDH / ECDSA and firmware integrity test

1.3 Operational Environment

The Module's operational environment is non-modifiable as defined by FIPS 140-2.

2. Cryptographic Functions and Critical Security Parameters (CSPs)

2.1 Supported Cryptographic Functions

The Module's cryptographic functions are outlined in Table 4.

Table 4. Approved Algorithms

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths/ Curves	Use
A1961	AES	FIPS 197, SP800-38A	OFB, CFB, CTR	128 256	Data Encryption and Decryption
A1961	RSA	FIPS 186-4, PKCS#1 v2.1	SHA-256, SHA-384 / RSASSA-PKCS1-v1_5, RSASSA-PSS	2048 3072	Digital Signature Generation
			SHA-1, SHA-256, SHA-384 / RSASSA-PKCS1-v1_5, RSASSA-PSS	2048 3072	Digital Signature Verification
			N/A	2048 3072	Key Generation
A1961	CVL	SP800-56Br2	RSA Decryption	2048 3072	Key Transport Primitive
A1961	KTS-RSA	SP800-56Br2	RSA Encryption and Decryption using RSAES_OAEP mode	2048 3072	Key Transport. The key establishment methodology provides between 112 and 128 bits of encryption strength

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths/ Curves	Use
Vendor Affirmed	CKG	SP800-133	Generation of symmetric keys and seeds when generating private keys for asymmetric key algorithm[1]	128 256	Key Generation
A1961	ECDSA	FIPS 186-4	SHA-256 SHA-384	P-256 P-384	Digital Signature Generation
			SHA-1 SHA-256 SHA-384		Digital Signature Verification
			N/A		Key Generation
			N/A		Public Key Validation
A1961	KAS-SSC	SP800-56A rev. 3	Full Unified, One Pass DH	P-256 P-384	Key Agreement
A1961	HMAC	FIPS 198-1	SHA-1 / HMAC SHA-256 / HMAC SHA-384 / HMAC	160 256 384	Keyed Message Digest for Message Authentication
A1961	SHS	FIPS 180-4	SHA-1 SHA-256 SHA-384	N/A	Message Digest
A1961	DRBG	SP800-90A	Block_Cipher_df	256	Conditioning Component
A1961	DRBG	SP800-90A	CTR_DRBG AES-256[2]	256	Deterministic Random Bit Generation

[1] The resulting symmetric key or generated seed is an unmodified output from the DRBG.
[2] The derivation function is not used during instantiation of the CTR_DRBG.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths/ Curves	Use
A1961	KBKDF	SP800-108	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384 / CTR[3]	N/A	Key Derivation
A1961	KTS	SP800-38F	HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 / CFB	128 256	Key transport based on the combination of AES (Cert. #A1961) and HMAC (Cert. #A1961). Key establishment methodology provides 128 or 256 bits ofencryption strength.
A1961	KDA	SP800-56C Rev. 1	SHA-1, SHA-256, SHA-384 / One-step	N/A	Key Derivation
ENT (P)	N/A	SP800-90B	N/A	N/A	Seeding/Reseeding the DRBG

2.2 Non-Approved, Not Allowed Algorithms

Table 5. Non-Approved, Not Allowed Algorithms

Function	Use
SHA-1	Digital signature generation[4]

[3] For algorithms TPM_ALG_KEYEDHASH and TPM_ALG_SYMCIPHER in [1], part 2.
[4] Digital signature generation with SHA-1 should not be used in an Approved Mode. For more details, refer to section 9.1.

3. Ports and Interfaces

The ports of the Module are:

- SPI Bus
- I2C Bus
- PP (Physical Presence) Pin
- Platform Reset
- Power

The logical interfaces and the mapping of the logical interfaces to the physical ports of the Module are described in the table below.

Table 6. Ports and Interfaces

Logical Interface	Description	Physical Ports
Control Input Interface	Control Input commands issued to the chip	SPI Bus I2C Bus PP pin Platform Reset Power
Status Output Interface	Status data output by the chip	SPI Bus I2C Bus
Data Input Interface	Data provided to the chip as part of the data processing commands	SPI Bus I2C Bus PP pin Platform Reset
Data Output Interface	Data output by the chip a part of the data processing commands	SPI Bus I2C Bus
Power Interface	Power interface of the chip	Platform Reset Power

The Module does not include a maintenance interface.

4. Roles, Authentication and Services

The three operation roles implemented by the Module are summarized in the table below.

Table 7. Roles

Role	Acronym	High Level Description
Crypto-Officer	CO	Also known as “Object Administrator”; installs and configures the Module, controls certification, changes authorization
Object User[5]	OU	Uses the object to execute services
Duplicate[6]	DUP	Duplicates an object (if object duplication is allowed)

The Module provides three authorization types to identify the role: Password, HMAC and Policy.

Password Authorization – A plaintext password value presented to authorize an action or identify a role. A plaintext password may be only appropriate for cases in which the path between the caller and the TPM is trusted or when the password is well known.

HMAC Authorization – Proving the knowledge of a shared secret via challenge-response HMAC protocol to authorize an action or identify a role. HMAC key is the shared secret.

Policy Authorization – Also known as “Enhanced Authorization”, allows entity-creators or administrators to require specific tests or actions to be performed as authorization method or identity proof. The specific policy is encapsulated in a digest value that is associated with an entity. An entity has a policy that defines the conditions for use of an entity. A policy may be arbitrarily complex. However, the policy is expressed as one (statistically unique) digest called the *authPolicy*.

Both HMAC and Policy authorizations include rolling nonce values as part of the protocol, as a challenge and to prevent a replay-attack.

Note: For commands that require Platform Authorization and commands that require a hierarchy authorization, it is possible to require an additional out-of-band authorization. This may use a dedicated pin in the TPM – also known as “Physical Presence” (PP). The TPM maintains a table of the commands that require that PP be asserted to authorize command execution. Only certain commands may be included in this table.

[5] For the context of FIPS 140-2, the Object User is mapped to the User role.
[6] For the context of FIPS 140-2, the Duplicate User is mapped to the Crypto-Officer role.

4.1 Authentication

4.1.1 Dictionary Attack (DA) Protection

The TPM incorporates mechanisms that provide protection against guessing or exhaustive searches of authorization values stored within the TPM.

The DA protection logic is triggered when the rate of authorization failures is too high. If this occurs, the TPM enters Lockout mode preventing any operation that requires use of a DA protected object. Depending on the settings of the configurable parameters, the TPM can "self-heal" after a specified amount of time or be programmatically reset using proof of knowledge of an authorization value or satisfaction of a policy (i.e., using lockoutAuth).

While authorization values that are expected to be high-entropy values will not need DA protection, lockoutAuth is always DA-protected even though it may have high-entropy.

4.1.2 Authorization Strength

The Module authenticates operator actions using authorization tokens. Considering the most conservative TPM command throughput on the bus and command execution duration, the number of commands that can be executed per second is 1,000, which is 60,000 attempts per minute.

4.1.2.1 Password and HMAC Authorization Strength

When a high-entropy authorization token is used (where DA protection may be disabled), each value, statistically, has the same probability to be chosen. For worst case scenario, assume SHA-1 output values size (160-bit array), producing 2^{160} different possible values.

Thus the probability for one randomly successful attempt is $2^{-160} = 6.8 * 10^{-49} < 10^{-48}$ which is less than the one in 1,000,000 maximum probability allowed by [3].

At maximum 60,000 trials per minute the probability for success in one minute is $2^{-160} \times 60{,}000 = 4.1 \times 10^{-44} < 10^{-43}$ which is less than the one in 100,000 maximum probability allowed by [3].

If a lower entropy authorization token is used (e.g., memorized PIN or password), a combination of password size (i.e., determines size of entropy) and DA protection setting should be selected to meet the FIPS requirements. A requirement of an 8-character password string with TCG's default DA settings[7] (maxTries = 3; recoveryTime = 1,000 seconds) would produce the necessary strength:

For the worst case, assume an eight-digit PIN, which has 10^8 different possible values. Thus the probability for one randomly successful attempt is 10^{-8} which is less than the one in 1,000,000 maximum probability allowed by [3].

The TCG default DA settings allow three trials before lockout (for duration of over a minute), so the probability for success in less than one minute in these settings would be $10^{-8} \times 3 < 10^{-7}$ which is less than the one in 100,000 maximum probability allowed by [3].

---

[7] See [1] part 1

4.1.2.2 Policy Authorization Strength

Since policy authorization is expressed as (statistically unique) digest, for worst case scenario, assume SHA-1 output values size (160-bit array), producing 2^{160} different possible values.

The probabilities for randomly successful single and multiple attempts are identical to those calculated in Section 4.1.2.1.

4.1.3 Authorization Token Value Selection

TPM permits the creation of objects with NULL authorization (empty buffer). However, to meet the Authorization Strength listed in Section 4.1.2, roles should not use NULL authorization values for CSPs.

The TPM Crypto-Officer's role is to set proper authorization values for the Storage and Endorsement hierarchies (if there is no OS managing these authorization values for the user).

The following calculations are done in the same manner as in Section 4.1.2.1.

For environments in which DA protection is disabled, a random 40-bit value is sufficient to meet the FIPS 140-2 requirement:

- The probability for one randomly successful attempt is $2^{-40} = 9.1 * 10^{-13} < 10^{-12}$ which is less than the one in 1,000,000 maximum probability allowed by [3].
- The probability for success in one minute is $2^{-40} \times 60{,}000 = 5.4 \times 10^{-8} < 10^{-7}$ which is less than the one in 100,000 maximum probability allowed by [3].

For environments in which DA protection is enabled and default values are used, a 7-digit PIN is sufficient to meet the FIPS 140-2 requirement:

- The probability for a randomly successful attempt is 10^{-7} which is less than the one in 1,000,000 maximum probability allowed by [3].
- The probability for success in one minute assuming three trials by DA protection would be: $10^{-7} \times 3 < 10^{-6}$ i.e. less than the one in 100,000 maximum probability allowed by [3].

4.2 Services

Table 8 lists all Module services, the affected CSPs, and the associated roles:

Table 8. Module Services

Service	Description	CSP	Role
Get Status	The Module implements a Get Status commands that returns the status of the Module, including success or failure of self tests. Note: This service (e.g., TPM2_GetCapability) does not require authentication	None	CO, OU, DUP
Self Tests	The Module runs power-on self tests automatically when powered on and on demand. Note: This service (e.g., TPM2_Selftest) does not require authentication	None	CO, OU, DUP
Encrypt	Used to encrypt data	Encryption keys, Public storage keys, Platform keys	CO, OU, DUP
Decrypt	Used to decrypt data	Encryption keys, Private storage keys, Endorsement keys, Platform keys	CO, OU
Zeroize	Used to zeroize (irreversibly destroy) Module's cryptographic keys and CSPs	Encryption keys, Public verification keys, Public storage keys, Private storage keys, Identity keys, HMAC keys, Endorsement keys, Platform keys, DRBG seed, DRBG Entropy Input, DRBG “V”, DRBG Key	CO
MAC, MAC Verify	Used to calculate and verify MAC for data	HMAC keys	CO, OU

Service	Description	CSP	Role
Key Generate	Used to generate keys	Encryption keys, Public verification keys, Public storage keys, Private storage keys, Identity keys, Ephemeral keys, HMAC keys, Endorsement keys, Platform keys, DRBG seed, DRBG Entropy Input, DRBG “V”, DRBG Key	CO, OU
RSA Verify	Used to verify data using RSA	Public verification keys, Platform keys, Firmware Update key	CO, OU
RSA Sign	Used to sign data using RSA	Identity keys, Platform keys	CO, OU
ECDSA Verify	Used to verify data using ECDSA	Public verification keys, Platform keys	CO, OU
ECDSA Sign	Used to sign data using ECDSA	Identity keys, Platform keys	CO, OU
Key Import	Used to import keys	Encryption keys, Public verification keys, Public storage keys, Private storage keys, Identity keys, HMAC keys, Platform keys	CO
Key Duplicate	Used to export keys	Encryption keys, Public storage keys, Private storage keys, Ephemeral keys, HMAC keys, Platform keys	CO, DUP
Key Agreement	Used to derive a key	Ephemeral Keys, Endorsement keys, Platform keys	CO, OU
TPM Identity	Used to authenticate TPM Identity to other parties	Identity keys	CO, OU

Service	Description	CSP	Role
TPM Endorsement	Used to prove to other parties that TPM is a genuine TPM	Endorsement keys	CO, OU
TPM Get Random	Used to generate random data Note: This service does not require authentication.	DRBG seed, DRBG Entropy Input, DRBG “V”, DRBG Key	CO, OU
TPM Stir Random	Used to add entropy to the random bit generator Note: This service does not require authentication.	DRBG seed, DRBG Entropy Input, DRBG “V”, DRBG Key	CO, OU
Install Module	Installs Module	HMAC keys, Platform keys	CO
Firmware Update	Updates Module’s firmware. Referred to in [1] as “Field Upgrade”. Requires Platform Authorization. Firmware that is loaded into the Module but is not within the scope of this validation requires a separate FIPS 140-2 validation [8].	Firmware Update key	CO

[8] For further information and instructions on the Firmware Update procedure, contact the platform manufacturer or Nuvoton support.

5. Key and CSP Management

Table 9 specifies each cryptographic key or CSP utilized by the Module.

For access type description, the following acronyms are used:

W - Write; the CSP is updated/written by the TPM

E - Execute; the CSP is used by the TPM for execution

TPM commands that have CSP as input/output parameters shall use parameter encryption.

Table 9. Cryptographic Keys

Key or CSP	Function	Usage	Service - Access
Encryption keys	AES KTS KBKDF DRBG CKG	Used to: - Wrap keys: for import/duplication, for wrapping keys stored outside the TPM and for session keys (audit or parameter encryption) - Encrypt/decrypt input/output parameters - Decrypt credentials Keys generated using DRBG, derived using KBKDF or securely transported using public/private storage keys.	Encrypt - E Decrypt - E Zeroize - W Key Import - E, W Key Generate - W Key Duplicate - E
Public verification keys	RSASA RSAKG ECDSA ECCKG DRBG	Used to verify signatures on data, as service for external application, or as part of Authorization Policy verification. Keys may be generated in the TPM (as part of Identity key generation) or loaded from external source.	Zeroize - W Key Generate - W RSA Verify - E ECDSA Verify - E Key Import - W
Public storage keys	KTS-RSA RSAKG KBKDF DRBG	Used to transport keys generated externally or generated by TPM. Keys may be generated in the TPM (as part of Private storage key generation) or imported from external source.	Encrypt - E Zeroize - W Key Generate - W Key Import - W Key Duplicate - E
Private storage keys	KTS-RSA RSAKG KBKDF KTS DRBG	Used to transport keys generated externally or generated by TPM. Keys may be generated in the TPM (stored encapsulated or wrapped outside the TPM) or imported from external source.	Decrypt - E Zeroize - W Key Generate - W Key Import - E, W Key Duplicate - E

Key or CSP	Function	Usage	Service - Access
Identity keys	RSASA RSAKG ECDSAE CCKG KBKDF KTS DRBG	Authorization tokens used to prove TPM identity to other parties. Used to sign information generated or controlled by the TPM. Keys may be generated in the TPM (stored encapsulated or wrapped outside the TPM) or imported from external source.	Zeroize - W Key Generate - W RSA Sign - E ECDSA Sign - E Key Import - W TPM Identity - E
Ephemeral keys	KAS-SSC ECCKG KBKDF KTS DRBG	Used to exchange secrets to establish a symmetric key, using One-Pass Diffie-Hellman. Used for: - Encryption of authorization session salt - Secret sharing for duplication - Secret sharing for credentials Keys may be generated in the TPM (stored encapsulated or wrapped outside the TPM) or imported from external source.	Key Generate - W Key Duplicate - E Key Agreement - E
HMAC keys	HMAC KTS DRBG CKG	Used to calculate and verify MAC codes for data. Used for: - Ensuring association of credential with a loaded object - Access or usage authorization - Symmetric signing - Audit Keys may be generated in the TPM (stored encapsulated or wrapped outside the TPM) or imported from external source.	Zeroize - W MAC, MAC Verify - E Key Generate - W Key Import - W Key Duplicate - E Install Module - W, E
Endorsement keys	KTS-RSA RSAKG KAS-SSC ECCKG KBKDF DRBG	Authorization tokens used to prove to the external parties that TPM is a genuine TPM. Keys may be generated in the TPM or installed during TPM manufacturing.	Decrypt - E Zeroize - W Key Generate - W Key Agreement - E TPM Endorsement - E

Key or CSP	Function	Usage	Service - Access
Platform keys	AES KTS-RSA RSASA RSAKG KAS-SSC ECDSA ECCKG KBKDF DRBG	Keys used by the Platform Firmware.	Encrypt - E Decrypt - E Zeroize - W Key Generate - W RSA Verify - E RSA Sign - E ECDSA Verify - E ECDSA Sign - E Key Import - E Key Duplicate - E Key Agreement - E Install Module - W, E
Firmware Update key	ECDSA	Used to verify signature on firmware updates. Key installed at the module manufacturing.	ECDSA Verify - E Firmware update - E
DRBG seed	ENT (P)	Used to seed the DRBG, generated by the ENT (P).	Zeroize - W Key Generate - E TPM Get Random - E TPM Stir Random - W
DRBG Entropy Input	ENT (P)	Used as Entropy input for the DRBG's seeds, generated by the ENT (P).	Zeroize - W Key Generate - E TPM Get Random - E TPM Stir Random - W
DRBG "V"	DRBG	CTR_DRBG's internal state that is updated each time another block length number of bits of output are produced.	Zeroize - W Key Generate - E
DRBG Key	DRBG	CTR_DRBG's Key.	Zeroize - W Key Generate - E

5.1 Key Generation and Entropy

The SP800-90A CTR_DRBG is seeded by the vetted conditioning component Block_Cipher_df, defined in SP800-90B; its input is 1024 bits extracted from ENT (P) with entropy of 512 bits (derived from the min-entropy which is 0.5). The result is that the DRBG is initialized at its full security strength of 256 bits, which is sufficient to support the strength of the largest key generated by the Module.

6. Self Tests

6.1 Power-On Self Tests

The Module implements the following tests during power-on:

Table 10. Power-On Self Tests (POST)

Cryptography Function	Test Type
Firmware integrity	HMAC using a 128-bit error detection code
HMAC	FIPS 198-1 KAT using SHA2-384
SHA-1, SHA2-256, SHA2-384	FIPS 180-4 KAT for each SHA type
AES Encryption / Decryption (CFB, CTR, OFB)	FIPS 197 KAT from SP800-38A
KBKDF	SP800-108 KAT
KDA	SP800-56C rev. 1 KAT per IG.D.8
DRBG	SP800-90A KAT
ENT (P)	SP800-90B RCT and APT Health Tests, running over 1024 consecutive samples

6.2 Conditional Self Tests

The Module implements the following conditional tests:

Table 11. Conditional Self Tests

Cryptography Function	Condition	Test Type
POST	TPM2_SelfTest(fullTest = YES) and in transition to Approved Mode 2	All tests listed in Table 11
ECDSA sign / verify	TPM2_SelfTest(fullTest = YES) and in transition to Approved Mode 2	FIPS 186-4 KAT
KAS-SSC	TPM2_SelfTest(fullTest = YES) and in transition to Approved Mode 2	SP800-56A rev. 3 KAT
RSA sign / verify	TPM2_SelfTest(fullTest = YES) and in transition to Approved Mode 2	PKCS#1v2.1, FIPS 186-4 KAT
RSA key generation	Key Generation	Conditional pair-wise consistency check for RSA public-private key pairs each time an RSA key pair is generated, using FIPS 186-4
ECC key generation	Key Generation	Conditional pair-wise consistency check for ECDSA public-private key pairs each time an ECDSA key pair is generated, using FIPS 186-4
Firmware Load Test	Firmware Update	Firmware update test during the firmware update. The digital signature is verified on the firmware image using an ECC (SHA2-256) algorithm, utilizing a 384-bit Firmware Update key
DRBG	New bits are generated	SP800-90A Continuous Self Test
ENT (P)	Upon first use of newly-generated bits	SP800-90B Health Test

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 may recover this error state if the power-on self test after reset or power-on succeeds.

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 140-2 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.

Module hardness testing was only performed at ambient room temperature; no assurance is provided for Level 3 hardness conformance at any other temperature.

8. Electromagnetic Interference and Compatibility (EMI/EMC)

The Module complies with the EMI/EMC requirements specified in Title 47, Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

9. Crypto-Officer Guidance

9.1 Modes of Operation

The TPM has three modes of operation:

1. Approved Mode 1: Described in Section 1.2.1
2. Approved Mode 2: Described in Section 1.2.2
3. Non-Approved Mode: This mode is entered once one of the functions listed in Table 5 is used as cryptographic function. Before entering this mode, all CSPs must be zeroized.

For FIPS Compliant mode, (Approved Mode 1 and Approved Mode 2), do not use functions listed in Table 5 as cryptographic functions.

9.2 Installation

To install the Module in the Approved Mode 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 ensures one-to-one binding with the platform.
- The platform on which 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.

9.3 Object Authorization

On object creation or changing object authorization, a password of at least eight characters shall be used. In addition, configure the module to enforce, at a minimum, a DA Setting policy where "maxTries" >=3 and "recoveryTime" >= 1,000.

9.4 Object Duplication

The TPM2_Duplicate command allows sending objects to/from the NULL hierarchy, which sends it off-chip unprotected. This is not allowed in FIPS 140-2.

The command has an attribute, "encryptedDuplication", which should always be SET in order to be compliant with FIPS 140-2. This requires an inner symmetric wrapping prior to the object receiving symmetric encryption to go off-chip. This also prevents the new parent from being TPM_RH_NULL (see [1], part 2).

When Object is created, set the attribute "encryptedDuplication" in the object.

9.5 Object Import

The TPM2_Import command allows importing objects from external modules. Import to the TPM only CSPs coming from FIPS-compliant modules in FIPS Compliant mode. In order to ensure that the sensitive area of the CSP being imported is encrypted, the CO should verify that the ‘encryptedDuplication’ attribute is SET for the object being imported.

10. Object User Guidance

The Object User shall follow the guidance in Sections 9.1, 9.3 and 9.5.

11. Duplicate Guidance

The Duplicate role shall follow the guidance in Section 9.4.

12. Acronyms

AES	Advanced Encryption Standard
CPU	Central Processing Unit
CSP	Critical Security Parameter
DA	Dictionary Attack
DRBG	Deterministic Random Bit Generator
ECC	Elliptic Curve Cryptography
EMC	Electro-Magnetic Compatibility
EMI	Electro-Magnetic Interference
FIPS	Federal Information Processing Standard
GPIO	General-Purpose Input Output bus
HMAC	Hash-based Message Authentication Code
I2C	Inter-Integrated Circuit bus
LPC	Low Pin Count bus
OTP	One-Time Programmable Memory
PCB	Printed Circuit Board
RAM	Random Access Memory
RSA	Rivest-Shamir-Adleman
SHS	Secure Hash Standard
SP800	NIST Special Publication (800 Series)
SPI	Serial Peripheral Interface bus
TCG	Trusted Computing Group
TIS	TPM Interface Specification
TPM	Trusted Platform Module

13. References

[1] TCG Trusted Platform Module Library Specification Family 2.0 Revision 1.59
https://www.trustedcomputinggroup.org/tpm-library-specification

[2] TCG PC Client Specific Platform TPM Profile (PTP) Specification for TPM Family 2.0 Revision 01.05 v14
https://trustedcomputinggroup.org/pc-client-platform-tpm-profile-ptp-specification

[3] FIPS 140-2
https://csrc.nist.gov/publications/detail/fips/140/2/final

Nuvoton provides comprehensive service and support.
For product information and technical assistance, contact the nearest Nuvoton center.

Important Notice

Nuvoton products are not designed, intended, authorized or warranted for use as components in systems or equipment intended for surgical implantation, atomic energy control instruments, airplane or spaceship instruments, transportation instruments, traffic signal instruments, combustion control instruments, or for other applications intended to support or sustain life. Furthermore, Nuvoton products are not intended for applications wherein failure of Nuvoton products could result or lead to a situation wherein personal injury, death or severe property or environmental damage could occur.

Nuvoton customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify Nuvoton for any damages resulting from such improper use or sales.

CONTACT INFORMATION

For Nuvoton Sales Offices in your region, visit us at:

https://www.nuvoton.com/buy/worldwide-sales-offices/

For Cloud Computing Product Line information, contact:

CloudComputing@nuvoton.com

Please note that all data and specifications are subject to change without notice.
All trademarks of products and companies mentioned in this document belong to their respective owners.

www.nuvoton.com