NUVOTON
TECHNOLOGY
CORPORATION

8 HASADNAOT STREET

HERZLIA, 46130

ISRAEL

NPCT6XX TPM 2.0

FIPS 140-2 SECURITY POLICY

DOCUMENT VERSION: 5.7

LAST REVISION: MAY 6, 2021

CONTENTS

LIST OF TABLES AND FIGURES

1. MODULE 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 Security Level 2.

The Module has two silicon revisions: FB5C85D and FB5C85E. The latter includes several issue fixes related to interface, power management and versioning. The changes have no impact on the security of the Module.

The FIPS 140-2 conformance testing was performed on the following configurations of the Nuvoton NPCT6xx TPM 2.0:

- FIRMWARE VERSIONS: 1.3.0.1, 1.3.1.0, 1.3.2.8
- HARDWARE VERSION 1: FB5C85D IN TSSOP28 PACKAGE
- HARDWARE VERSION 2: FB5C85D IN QFN32 PACKAGE
- HARDWARE VERSION 3: FB5C85E IN TSSOP28 PACKAGE
- HARDWARE VERSION 4: FB5C85E IN QFN32 PACKAGE

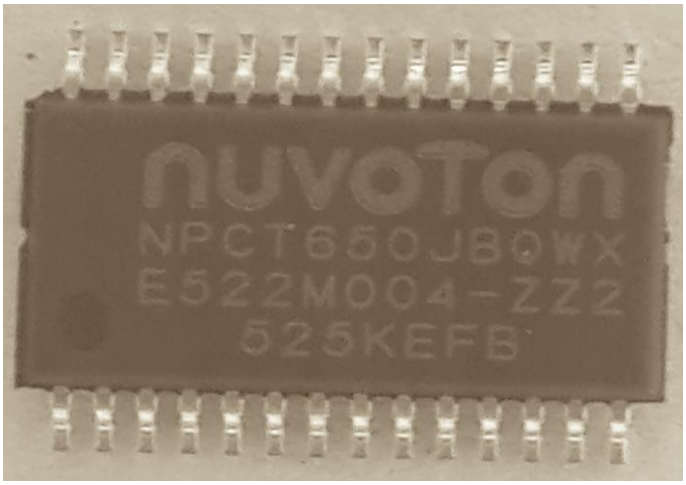
Images depicting the Module are shown in Figure 1:

FIGURE 1: TPM 2.0 IMAGES

FB5C85D IN TSSOP28 PACKAGE

FB5C85D IN QFN32 PACKAGE

FB5C85E IN TSSOP28 PACKAGE

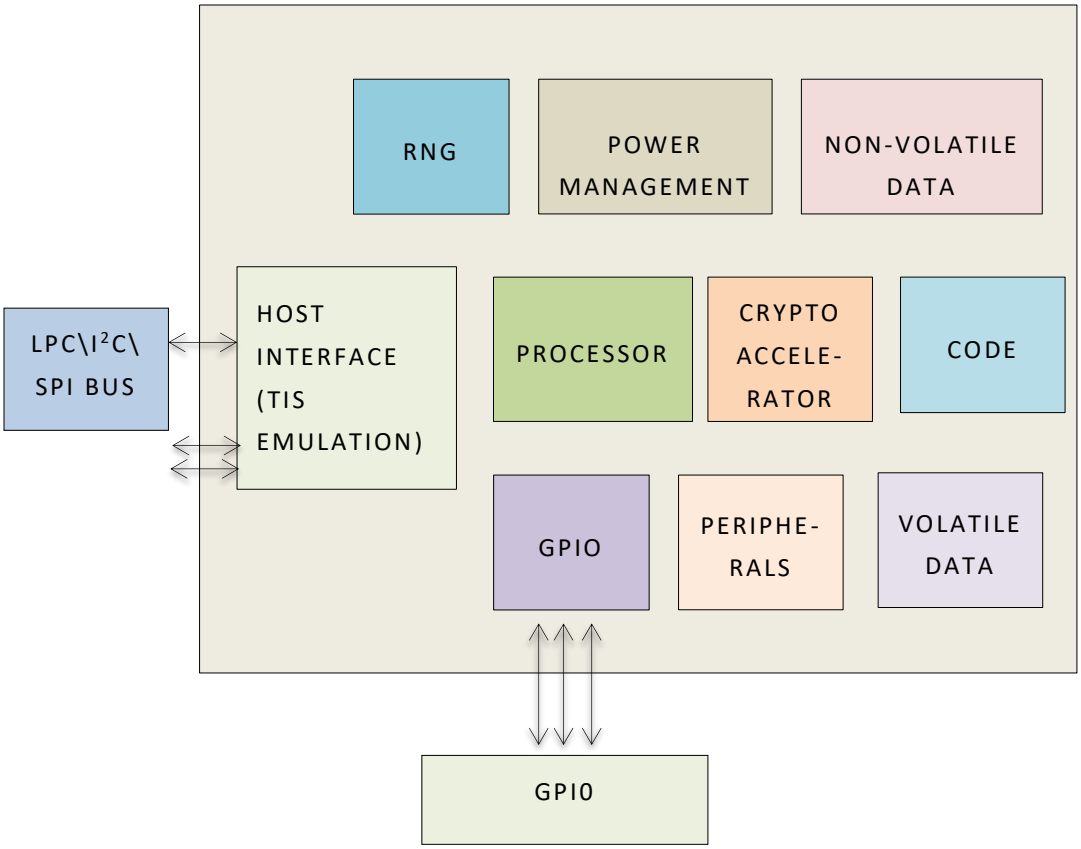


FB5C85E IN QFN32 PACKAGE

The PHYSICAL CRYPTOGRAPHIC BOUNDARY of the Module is the outer boundary of the chip packaging.

A LOGICAL DIAGRAM of the Module is shown in Figure 2:

FIGURE 2: 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	2
Operating Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

2. CRYPTOGRAPHIC FUNCTIONS

The Module's cryptographic functions are outlined in Table 2.

TABLE 2: CRYPTOGRAPHIC FUNCTIONS

FUNCTION	KEYSIZE	USE	CERT NUMBER
APPROVED FUNCTIONS			
AES MODES: ECB (ENCRYPT), OFB (ENCRYPT/DECRYPT), CFB128(ENCRYPT/DECRYPT), CTR (ENCRYPT)	128 BITS	ENCRYPTION AND DECRYPTION	3541 3542
RSA SIGNATURE GENERATION AND VERIFICATION USING RSASSA-PKCS1-V1_5 AND RSASSA-PSS MODES AND SHA-1/SHA-256	1024 & 2048 BITS	DIGITAL SIGNATURE VERIFICATION	1819 1820
ECDSA SIGNATURE GENERATION AND VERIFICATION USING P-256 CURVE AND SHA-1/SHA-256	256 BITS	DIGITAL SIGNATURES	719 720

HMAC KEYED HASH USING SHA-1 AND SHA-256	160 BITS, 256 BITS	KEYED MESSAGE DIGEST	2262 2263
SHS HASH USING SHA-1 AND SHA-256	160 BITS, 256 BITS	MESSAGE DIGEST	2919 2920
GENERATION OF RSA KEYS FIPS 186-4	2048 BITS	KEY PAIR GENERATION	1819 1820
GENERATION OF ECDSA KEYS FIPS 186-4	256 BITS	KEY PAIR GENERATION	719 720
ECC KEY AGREEMENT USING P-256 CURVE AND SHA-256	256 BITS	KEY AGREEMENT	66 67
SP 800-90A DRBG	N/A	RANDOM NUMBER GENERATION & SYMMETRIC KEY GENERATION	898 899
APPROVED SERVICES			
CVL SP 800-135 REV1	N/A	TPM KEY DERIVATION	594 596
CVL SP 800-56A REV. 3 USING P-256 CURVE	N/A	TPM KEY DERIVATION	VENDOR AFFIRMED
ALLOWED FOR USE FUNCTIONS			
RSA KEY WRAPPING	2048 BITS	WRAP &	N/A

		Unwrap symmetric keys	
NDRNG (entropy source).	N/A	Generate the seed input for the DRBG	N/A

In the Approved mode of operation, the Module supports a key size of 2048 bits for RSA key wrapping. This is equivalent to a key strength of 112 bits. AES key wrapping functionality is compliant with SP 800-38F Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping since it uses an Approved symmetric encryption algorithm (AES #3541 and #3542) with an Approved authentication technique (HMAC #2262 and #2263). This is designated as KTS (AES Certs. #3541 and #3542 and HMAC Certs. #2262 and #2263) on the certificate.

Note: Neither the TLS protocol nor the TPM protocol were tested by the CAVP or CMVP.

2.1 Non-Approved, Allowed Function

The module supports the following Non-Approved but Allowed functions, as listed in Table 2:

- RSA Key Wrapping; key size is 2048 bits
- NDRNG (proprietary Non-Deterministic Hardware RNG); available entropy is 256 bits

2.2 Non-Approved, Non-Allowed Function

The Module supports signature generation using RSA-SHA-1. This function is Non-Approved and is considered equivalent to plaintext or obfuscation.

3. PORTS AND INTERFACES

The physical ports of the Module are

- LPC Bus
- SPI Bus
- I2C Bus
- GPIO Bus

The logical interfaces and the mapping of the logical interfaces to the physical ports of the Module are described in Table 3.

TABLE 3: PORTS AND INTERFACES

LOGICAL INTERFACE	DESCRIPTION	PHYSICAL PORTS
CONTROL INPUT INTERFACE	CONTROL INPUT COMMANDS ISSUED TO THE CHIP	LPC BUS SPI BUS I2C BUS GPIO BUS
STATUS OUTPUT INTERFACE	STATUS DATA OUTPUT BY THE CHIP	LPC BUS SPI BUS I2C BUS GPIO BUS
DATA INPUT INTERFACE	DATA PROVIDED TO THE CHIP AS PART OF THE DATA PROCESSING COMMANDS	LPC BUS SPI BUS I2C BUS GPIO BUS
DATA OUTPUT INTERFACE	DATA OUTPUT BY THE CHIP A PART OF THE DATA PROCESSING COMMANDS	LPC BUS SPI BUS I2C BUS GPIO BUS
POWER INTERFACE	POWER INTERFACE OF THE CHIP	POWER PIN GROUND PIN

The Module does not include a maintenance interface.

4. ROLES AND SERVICES

The OPERATOR ROLES implemented by the Module are summarized in Table 4.

TABLE 4: ROLES

ROLE	HIGH LEVEL DESCRIPTION
CRYPTO OFFICER	INSTALLS AND CONFIGURES THE PRODUCT, EXECUTES CRYPTO ALGORITHMS AND GENERATES KEYS
USER	EXECUTES CRYPTO ALGORITHMS AND GENERATES KEYS

The Module provides the set of SERVICES described in Table 5. For each service, the table includes a description of the service and lists the roles for which the service is available.

The Module implements authentication to authenticate operator actions using authentication tokens. The authentication token length is 32 bytes. Therefore, the total number of authentication token combinations is 2^256 = 10^77, which meets the authentication strength requirements of FIPS 140-2.

The maximum number of authentication attempts before lockout is 10. The recovery time is 7,200 seconds (2 hours), and the lockout recovery time is 86,400 seconds (24 hours). Since only 10 tries are allowed, the probability of a successful random attempt during a one minute period is 10 / 2^256, which is less than one in 100,000.

The Module stores all authentication results in volatile memory, which is cleared when the Module is powered off.

The Module always encrypts cryptographic key on key input and output, which meets the key encryption requirements of FIPS 140-2 and Security Level 2.

The Module provides SP 800-90A DRBG random bit generation services without authentication, as permitted by FIPS 140-2 Implementation Guidance.

TABLE 5: SERVICES

SERVICE	DESCRIPTION	ROLE
GET STATUS	THE MODULE IMPLEMENTS A GET STATUS COMMAND THAT RETURNS THE STATUS OF THE MODULE, INCLUDING SUCCESS OR FAILURE OF SELF-TESTS. **NOTE**: THIS SERVICE DOES NOT REQUIRE AUTHENTICATION	CRYPTO OFFICER USER
RUN SELF-TESTS	THE MODULE RUNS POWER-UP SELF-TESTS AUTOMATICALLY WHEN POWERED ON. ONE CAN EXECUTE SELF-TESTS ON DEMAND BY POWER-CYCLING THE MODULE.	CRYPTO OFFICER USER
ENCRYPT	USED TO ENCRYPT DATA	CRYPTO OFFICER USER
DECRYPT	USED TO DECRYPT DATA	CRYPTO OFFICER USER
ZEROIZE	USED TO ZEROIZE (IRREVERSIBLY DESTROY) MODULE'S CRYPTOGRAPHIC KEYS AND CSPS. THE KEYS AND CSPS STORED IN THE NON-VOLATILE AND VOLATILE MEMORY ARE ZEROIZED BY EXECUTING THE CORRESPONDING KEY/ENTITY ZEROIZATION COMMANDS: 1. TPM2_FLUSHCONTEXT 2. TPM2_CLEAR	CRYPTO OFFICER USER

MAC & MAC Verify	Used to calculate and verify MAC for data	Crypto Officer User
Key Generate	Used to generate keys	Crypto Officer User
RSA Verify	Used to verify data using RSA	Crypto Officer User
ECDSA Verify	Used to verify data using ECDSA	Crypto Officer User
ECDSA Sign	Used to sign data using ECDSA	Crypto Officer User
RSA Wrapping & Unwrapping	Used to wrap & unwrap cryptographic keys using RSA	Crypto Officer User
Key Import	Used to import keys	Crypto Officer User
Key Agreement	Used to derive a key	Crypto Officer User
TPM Identity	Used to authenticate TPM Identity to other parties	Crypto Officer User
TPM Endorsement	Used to prove to other parties that TPM is a genuine TPM	Crypto Officer User

TPM GET RANDOM	USED TO GENERATE RANDOM DATA **NOTE**: THIS SERVICE DOES NOT REQUIRE AUTHENTICATION	CRYPTO OFFICER USER
TPM STIR RANDOM	USED TO ADD ENTROPY TO THE RANDOM BIT GENERATOR	CRYPTO OFFICER USER
INSTALL MODULE	INSTALLS MODULE	CRYPTO OFFICER
FIRMWARE UPDATE	UPDATES MODULE'S FIRMWARE	CRYPTO OFFICER USER

5. KEY MANAGEMENT

Table 6 specifies each cryptographic key utilized by the Module. For each key, the table provides a description of its use; derivation or import; and storage.

NOTE: **READ** is defined as read access; **WRITE** is defined as write access.

TABLE 6: CRYPTOGRAPHIC KEYS

KEY OR CSP	USAGE	SERVICE & ACCESS	ORIGIN & STORAGE
AES SYMMETRIC ENCRYPTION KEYS	USED TO ENCRYPT AND DECRYPT DATA	ENCRYPT READ DECRYPT READ KEY GEN WRITE KEY WRAPPING /UNWRAPPING WRITE KEY IMPORT WRITE ZEROIZE WRITE	GENERATED OR IMPORTED BY THE MODULE, STORED IN OTP OR IN NON-VOLATILE FLASH IN PLAINTEXT

RSA and ECDSA public verification keys	Used to verify signatures on data	RSA Verify READ Key Gen WRITE Zeroize WRITE Key Wrapping /Unwrapping WRITE Key Import WRITE	Generated or imported by the Module, stored in volatile RAM or in non-volatile flash in plaintext
RSA public storage keys	Used to wrap symmetric keys	RSA Wrap/Unwrap READ Key Import WRITE RSA Key Gen WRITE Zeroize WRITE	Generated or imported by the Module, stored in volatile RAM or in non-volatile Flash in plaintext

RSA private storage keys	Used to unwrap symmetric keys	RSA Wrap/Unwrap READ RSA Key Gen WRITE Key Import WRITE Zeroize WRITE	Generated or imported by the Module, stored in volatile RAM or in non-volatile Flash in plaintext
identity keys	Authentication tokens used to prove TPM identity to other parties	TPM Identity READ RSA Key Gen WRITE Key Import WRITE Zeroize WRITE	Generated or imported by the Module, stored in volatile RAM or in non-volatile Flash in plaintext
RSA private binding keys	Used to unbind (unwrap) a key bound by an external entity	Data Binding READ RSA Key Gen WRITE Zeroize WRITE	Generated or imported by the Module, stored in volatile RAM or in non-volatile Flash in plaintext

HMAC keys	Used to calculate and verify MAC codes for data	MAC/MAC Verify READ Key Gen READ Key Import WRITE Zeroize WRITE	Generated or imported by the Module, stored in volatile RAM or in non-volatile Flash in plaintext
DRBG seeds	Used to seed the DRBG	Key Gen READ RSA Key Gen READ Zeroize WRITE	Generated by the Module using the non-Approved non-deterministic hardware RNG (entropy source) stored in volatile RAM in plaintext
Endorsement Keys	Authentication tokens used to prove to the external parties that TPM is a genuine TPM	TPM Endorsement READ	Generated by the Module

Platform Keys	Keys used by the Platform Firmware	RSA Key Gen WRITE ECDSA Key Gen WRITE	Generated by the Module
HMAC Authentication Key	Used for HMAC authentication of data	Key Generate WRITE MAC/MAC Verify READ	Generated by the Module
Firmware Update Key	Used to verify signature on firmware updates	Firmware update READ	Installed at the factory

6. POWER-ON SELF TESTS

The Module implements a power-up integrity check using a 256-bit error detection code.

The Module implements power-up cryptographic algorithm tests that are described in Table 7.

TABLE 7: SELF-TESTS

CRYPTO FUNCTION	TEST TYPE
AES CTR ENCRYPT (ALL MODES) AND DECRYPT (ALL MODES)	KNOWN ANSWER TEST (ENCRYPT AND DECRYPT)
RSA VERIFY	KNOWN ANSWER TEST (VERIFY)
ECDSA SIGN/VERIFY	PAIR-WISE CONSISTENCY TEST
ECC KEY AGREEMENT	PAIR-WISE CONSISTENCY TEST
HMAC KEYED HASH	KNOWN ANSWER TEST (KEYED HASH)
SHS HASH	KNOWN ANSWER TEST (HASH)
DRBG RANDOM NUMBER GENERATION	KNOWN ANSWER TEST (GENERATE RANDOM BLOCK)

7. CONDITIONAL SELF-TESTS

The Module executes the following tests and checks:

- Continuous DRBG test on each execution of the SP 800-90A DRBG (both the entropy source and the approved algorithm are tested).
- Conditional pair-wise consistency check for RSA public-private key pairs each time an RSA key pair is generated, using FIPS 186-4 key pair generation algorithm.
- Conditional pair-wise consistency check for ECDSA public-private key pairs each time an ECDSA key pair is generated, using FIPS 186-4 key pair generation algorithm.
- Firmware update test during the firmware update. The digital signature is verified on the firmware image using an RSA (SHA-256) algorithm, utilizing a 2048-bit firmware update key.

If any of the conditional or power-on self-tests fail, the Module enters an error state where both data output and cryptographic services are disabled.

In addition, the Module executes DRBG Instantiate, DRBG Generation, DRBG reseed, and DRBG Instantiate tests, as prescribed by SP 800-90A.

8. CRYPTO-OFFICER GUIDANCE

To install the Module in the Approved Mode of operation, the following steps must be followed:

- The Module must be physically controlled during the installation.
- The Module must be placed on the PCB as described in the Module technical specifications.
- The Module arrives from the manufacturer, typically pre-configured with FIPS mode enabled according to the *NPCT65x TPM2.0 Programmer's Guide* (CFG_H[0] is zero). If the initialization sequence was not executed by the manufacturer, the Crypto Officer must initialize the Module using the NTC2_PreConfig command (see Section 3.1 in the *NPCT65x TPM2.0 Programmer's Guide*).

9. USER GUIDANCE

The user shall take security measures to protect the tokens used to authenticate the user to the Module.

10. ACRONYMS

AES	Advanced Encryption Algorithm
CPU	Central Processing Unit
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
DRBG	Deterministic Random Bit Generator
RSA	Rivest-Shamir-Adleman
SHS	Secure Hash Standard
SP	Special Publication
SPI	Serial Peripheral Interface bus
TCG	Trusted Computing Group
TIS	TPM Interface Specification
TPM	Trusted Platform Module

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

Headquarters

No. 4, Creation Rd. 3
Science-Based Industrial Park
Hsinchu, Taiwan, R.O.C
TEL: 886-3-5770066
FAX: 886-3-5665577
http://www.nuvoton.com.tw (Ch.)
http://www.nuvoton.com (Eng.)

Nuvoton Technology Corporation America

2727 North First Street
San Jose, CA 95134, U.S.A.
TEL: 1-408-9436666
FAX: 1-408-5441798

Nuvoton Technology (Shanghai) Ltd.

27F, 2299 Yan An W. Rd.
Shanghai, 200336 China
TEL: 86-21-62365999
FAX: 86-21-62365998

Taipei Office

1F, No.192, Jingye 1st Rd
Zhongshan District, Taipei, 104
Taiwan, R.O.C.
TEL: 886-2-2658-8066
FAX: 886-2-8751-3579

Winbond Electronics Corporation Japan

NO. 2 Ueno-Bldg., 7-18, 3-chome
Shinyokohama Kohoku-ku
Yokohama, 222-0033
TEL: 81-45-4781881
FAX: 81-45-4781800

Nuvoton Technology (H.K.) Ltd.

Unit 9-15, 22F, Millennium City 2
378 Kwun Tong Rd
Kowloon, Hong Kong
TEL: 852-27513100
FAX: 852-27552064

For Advanced PC Product Line information contact: APC.Support@nuvoton.com