NUVOTON
TECHNOLOGY
CORPORATION

8 HASADNAOT STREET

HERZLIA, 46130

ISRAEL

NPCT6XX TPM 1.2

FIPS 140-2 SECURITY POLICY

DOCUMENT VERSION: 4.4

LAST REVISION: AUGUST 9, 2016

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 import 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 the commercial-grade specifications for power, temperature, reliability, shock, and vibrations.

The FIPS 140-2 conformance testing was performed on two platforms specified below

NUVOTON NPCT6XX TPM 1.2

FIRMWARE VERSIONS: 5.81.0.0, 5.81.1.0, 5.81.2.1

HARDWARE VERSION 1: FB5C85D IN TSSOP28 PACKAGE

HARDWARE VERSION 2: FB5C85D IN QFN32 PACKAGE

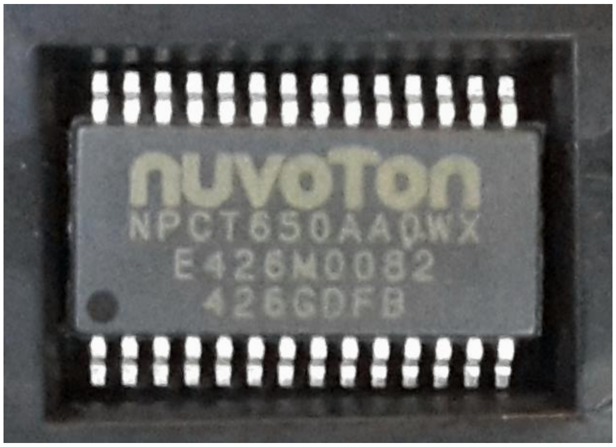
HARDWARE VERSION 3: FB5C85E IN TSSOP28 PACKAGE

HARDWARE VERSION 4: FB5C85E IN QFN32 PACKAGE

Images depicting the Module are provided on the next page.

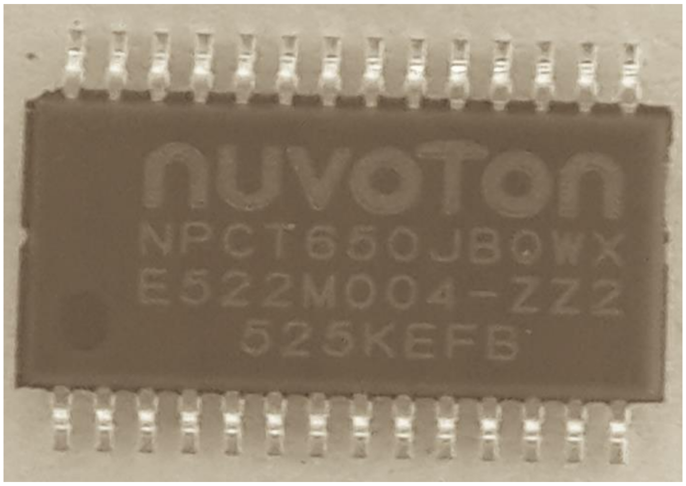
FIGURE 1: TPM 1.2 IMAGES

FB5C85D IN TSSOP28 PACKAGE



FB5C85D IN QFN32 PACKAGE

FB5C85E IN TSSOP28 PACKAGE

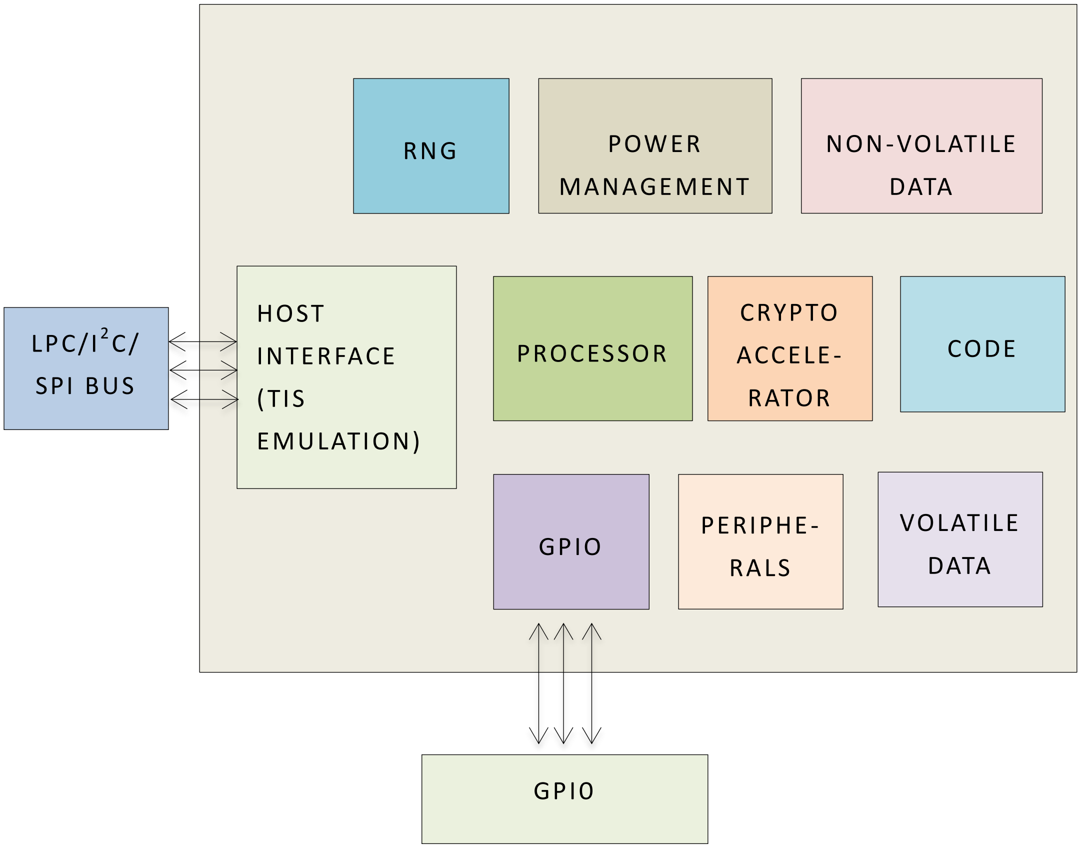


FB5C85E IN QFN32 PACKAGE

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

A LOGICAL DIAGRAM of the Module is provided on the next page.

FIGURE 2: TPM 1.2 LOGICAL BLOCK DIAGRAM



The Module was tested to meet OVERALL SECURITY LEVEL 1 of the FIPS PUB 140-2 standard. The Security Level as per each section of FIPS PUB 140-2 is specified in the table on the next page.

TABLE 1: SECURITY LEVELS

FIPS 140-2 SECTION	**SECURITY LEVEL**
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	1
Operating Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

2. CRYPTOGRAPHIC FUNCTIONS

The cryptographic functions of the Module are outlined in the table below.

TABLE 2: CRYPTOGRAPHIC FUNCTIONS

FUNCTION	KEYSIZE	USE	CERT NUMBER
APPROVED FUNCTIONS			
AES ENCRYPT MODES: ECB, CTR	128 BITS	ENCRYPTION	3093 3468
RSA VERIFY	1024 & 2048 BITS	DIGITAL SIGNATURE VERIFICATION	1582 1779
HMAC KEYED HASH HMAC-SHA-1	160 BITS	KEYED MESSAGE DIGEST	1938 2213
SHS HASH	N/A	MESSAGE DIGEST	2554 2863
APPROVED SERVICES			
CVL SP 800-135 REV1	N/A	TPM KEY DERIVATION	373 535

Allowed for use functions			
RSA Key Wrapping	2048 bits	Wrap & Unwrap symmetric keys	N/A
Hardware-based non-Approved non-deterministic RNG (entropy source).	N/A	Generate seed & the seed key for the RNG	N/A

In the Approved mode of operation the Module supports key size of 2048 bits for RSA key wrapping, which corresponds to the effective key strength of 112 bits.

The module supports key wrapping using the AES algorithm.

Note: no TPM protocol has been used or tested by the CAVP and CMVP.

2.1 Non-Approved Non-Allowed Functions

The Module supports signature generation using RSA-SHA-1, which is used in the TPM IDENTITY service. This function is Non-Approved and is considered equivalent to plaintext or obfuscation. The module also supports a disallowed FIPS 186-2 RNG.

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 the table below.

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 the table below.

TABLE 4: ROLES

ROLE	HIGH LEVEL DESCRIPTION
CRYPTO OFFICER	INSTALLS AND CONFIGURES THE PRODUCT AND MANAGES USERS
USER	EXECUTES CRYPTO ALGORITHMS AND ESTABLISHES KEYS

The Module provides a set of SERVICES described in the table on the next page. For each service the table includes a description of the service, as well as lists roles in which the service is available.

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.	Crypto Officer
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
Encrypt	Used to encrypt data	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: - TPM_FlushSpecific - TPM_OwnerClear	Crypto Officer
MAC & MAC Verify	Used to calculate and verify MAC for data	User
RSA Verify	Used to verify data using RSA	User
RSA Wrap & Unwrap	Used to wrap & unwrap cryptographic keys using RSA	User
Key Import	Used to import keys	User

TPM Identity	Used to authenticate TPM Identity to other parties	User
TPM Endorsement	Used to prove to other parties that TPM is a genuine TPM	User
Unbinding	Used to unbind symmetric keys using RSA Private Binding Key	User
TPM Get Random	Used to generate random data	User
TPM Stir Random	Used to add entropy to the random bit generator	User
Install Module	Installs module	Crypto Officer
Firmware Update	Updates module's firmware	Crypto Officer

5. KEY MANAGEMENT

The table below 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 DATA	ENCRYPT READ KEY WRAP/UNWRAP WRITE KEY IMPORT WRITE ZEROIZE WRITE	IMPORTED BY THE MODULE, STORED IN OTP OR IN NON-VOLATILE FLASH IN PLAINTEXT
RSA PUBLIC VERIFICATION KEYS	USED TO VERIFY SIGNATURES ON DATA	RSA VERIFY READ ZEROIZE WRITE KEY WRAP/UNWRAP WRITE KEY IMPORT WRITE	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 Zeroize WRITE	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 Key Import WRITE Zeroize WRITE	Imported by the Module, stored in volatile RAM or in non-volatile Flash in plaintext
identity keys	Authentication tokens used to TPM identity to other parties	TPM Identity READ Key Import WRITE Zeroize WRITE	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 Zeroize WRITE	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	imported by the Module, stored in volatile RAM or in non-volatile Flash in plaintext
Endorsement Key	Authentication token used to prove to the external parties that TPM is a genuine TPM	TPM Endorsement READ	Installed at the factory
Firmware Update Key	Used to verify signature on firmware updates	Firmware update READ	Installed at the factory

The key zeroization service is executed by running the following two commands in sequence:

- TPM_FlushSpecific
- TPM_OwnerClear

All keys and CSPs that are subject to the key zeroization requirements of FIPS 140-2 are zeroized by executing the key zeroization service.

The module implements power-up cryptographic algorithm tests that are described in the table below.

6. POWER-ON SELF TESTS

The Module implements a power-up integrity check using a 128-bit error detection code.

The module implements power-up cryptographic algorithm tests that are described in the table below.

TABLE 7: SELF-TESTS

CRYPTO FUNCTION	TEST TYPE
AES CTR ENCRYPT	KNOWN ANSWER TEST (ENCRYPT)
RSA VERIFY	KNOWN ANSWER TEST (VERIFY)
HMAC KEYED HASH	KNOWN ANSWER TEST (KEYED HASH)
SHS HASH	KNOWN ANSWER TEST (HASH)
RNG RANDOM NUMBER GENERATION	KNOWN ANSWER TEST (GENERATE RANDOM BLOCK)

7. CONDITIONAL SELF-TESTS

The Module executes continuous RNG test on each execution of the FIPS 186-2 RNG.

The Module executes continuous RNG test on each execution of the non-Approved hardware non-deterministic RNG (entropy source).

The Module executes 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.

The module executes the 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.

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 normally would come from the manufacturer pre-configured with *TpmInit* script already executed. If the initialization sequence has not been executed by the manufacturer, the Crypto Officer shall initialize the module as described in Nuvoton "NPCT6xx Initialization and Configuration" document. This includes running the *TpmInit* script with the *-fips* flag.

9. USER GUIDANCE

The user shall not generate keys using the disallowed RNG but shall instead use the Key Import service.

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

NOTE: Authentication is not covered by the FIPS 140-2 Level 1 requirements.

10. ACRONYMS

AES	Advanced Encryption Algorithm
CPU	Central Processing Unit
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
RNG	Random Number 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 (Chinese)
http://www.nuvoton.com English)

Nuvoton Technology Corporation America
2727 North First Street
San Jose, CA 95134, U.S.A.
TEL: 1-408-544-1718
FAX: 1-408-544-1787

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
Taiwan City 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

www.nuvoton.com