FIPS 140-2 Security Policy

for

Nuvoton Technology Corporation

Nuvoton TPM 1.2

Hardware Version: FD5C37
Firmware version: 4.1.5

Document Version: 1.13

Last Revision: Sep 10 2013

Table of Contents

Contents

List of Tables

1. General

Nuvoton Trusted Platform Module is a hardware cryptographic module, which 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, which provides cryptographic services utilized by external applications.

The module meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations.

The module models used for the testing are as follows:

- Nuvoton TPM 1.2

  Hardware version: FD5C37
  Firmware version: 4.1. 5

Note: the model designation above corresponds to one single model of the product.

An image depicting the module is provided below.

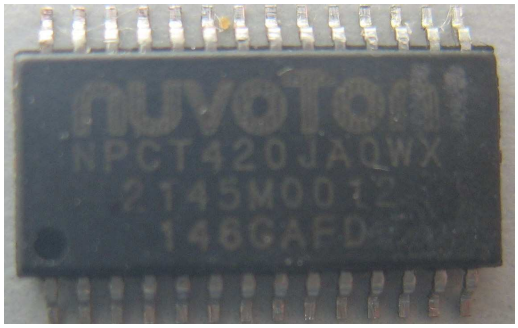

Figure 1: Hardware and Physical Cryptographic Boundary

The physical security boundary of the module is the outer boundary of the chip packaging.

A logical diagram of the module is provided below

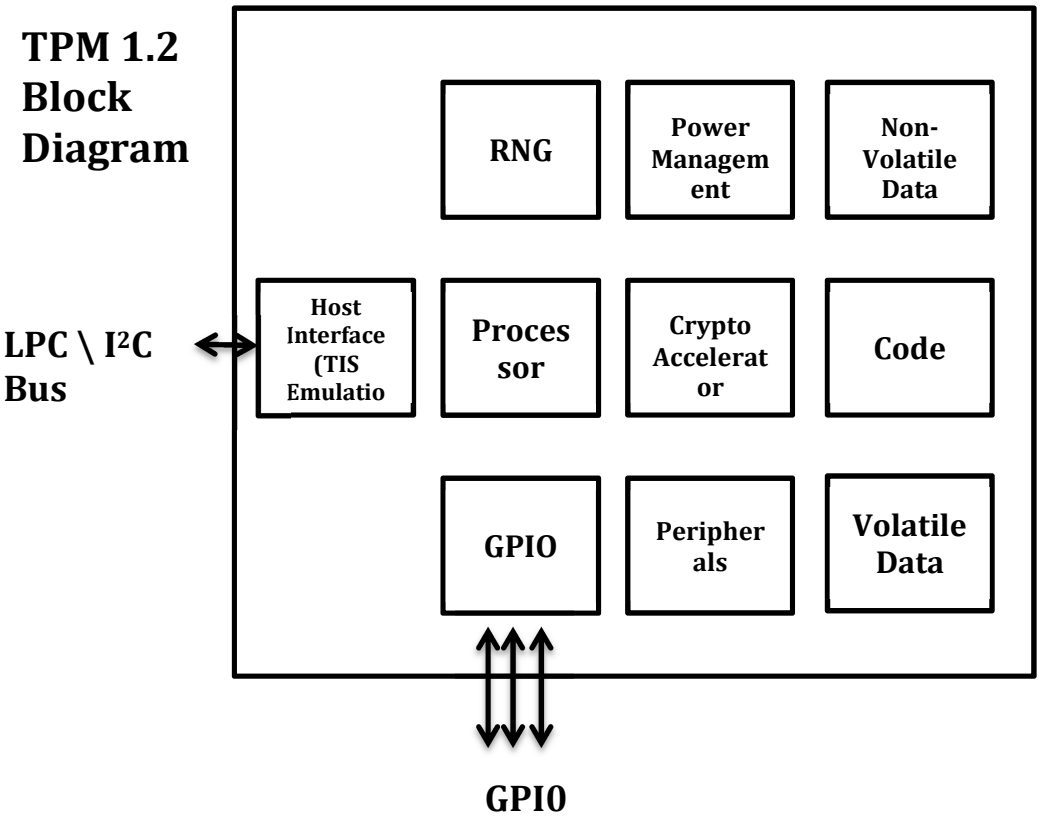

Figure 2: Logical Diagram

The module was tested to meet overall Security Level 1 of the FIPS 140-2 standard. The Security Level per FIPS 140-2 section is specified below

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

Table 1. Security Levels

2. Cryptographic Functions.

The module implements the following Cryptographic Functions.

Cryptographic Function	Key Size	Use	Certificate Number
Approved Functions			
AES encrypt Modes: ECB, CTR	128 bits	Encryption	#2354
RSA sign/verify	1024 bits, 2048 bits	Digital Signatures	#1215
SHS hash SHA-1	N/A	Message Digest	#2028
HMAC keyed hash HMAC-SHA-1	160 bits	Keyed Message Digest	#1460
FIPS 186-3 Generation of RSA Keys	2048	Key Pair Generation	#1215
FIPS 186-2 RNG	N/A	Random number generation, generation of symmetric keys	#1174
Approved Services			
CVL (SP 800-135 rev1)			#59
Allowed for use functions			
RSA Key Wrapping	1024, 2048 bits	Wrap/Unwrap symmetric keys	N/A
Hardware-based non-Approved non-deterministic RNG (entropy source).	N/A	Obtain the seed and the seed key for the FIPS 186-2 RNG.	N/A

Table 2. Cryptographic Functions.

In the Approved mode of operation the module supports key sizes from 1024 or 2048 bits for RSA key wrapping, which corresponds to the effective key strength from 80 or 112 bits.

3. Ports and Interfaces.

The physical ports of the module are I2C Bus, LPC Bus.

The logical interfaces and their mapping to physical ports of the module are described below

Logical Interface	*Description*	*Physical Port(s)*
Control Input Interface	**Control Input commands issued to the chip**	I2C Bus/LPC Bus
Status Output Interface	**Status data output by the chip**	I2C Bus/LPC Bus
Data Input Interface	**Data provided to the chip as part of the data processing commands**	I2C Bus/LPC Bus
Data Output Interface	**Data output by the chip a part of the data processing commands**	I2C Bus/LPC Bus
Power Interface	**Power interface of the chip**	Power and ground pins

Table 3 Interfaces and ports

The module does not include a maintenance interface.

4. Roles, Services and Authentication

The services provided by the module do not require authentication.

The module always runs in the Approved mode of operation.

The module implements the following roles:

Role	High Level Description
Crypto Officer	Installs and configures the product, manages users
User	Executes crypto algorithms and generates keys

Table 4. Roles.

The module provides a set of services described below. For each service, a description of the service is provided and roles in which the service is available are specified.

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 the module is powered on. One can execute self-tests on demand by power-cycling the module	Crypto Officer
Encrypt	Encrypt data	User
Zeroize	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 key/entity zeroization commands TPM_FlushSpecific TPM_OwnerClear	Crypto Officer

Service	Description	Role
MAC / MAC Verify	Calculate/Verify MAC for data	User
Key Generate	Generate symmetric encryption keys or HMAC keys	User
RSA Sign/Verify	Sign/Verify data using RSA	User
RSA Wrap /Unwrap	Wrap/Unwrap cryptographic keys using RSA	User
RSA Key Generate	Generate RSA public-private key pairs	User
Key Import	Import wrapped symmetric keys and public-private keys pairs	User
TPM Identity	Authenticate TPM Identity to other parties	User
TPM Endorsement	Prove to other parties that TPM is a genuine TPM	User
Unbinding	Unbind symmetric keys using RSA Private Binding Key	User
TPM Get Random	Get random data	User
TPM Stir Random	Add entropy to the random bit generator	User
Install Module	Install Module	Crypto Officer

Table 5. Services.

5. Cryptographic Key Management.

The table below specifies each cryptographic key utilized by the module. For each key the table provides a description of its use and derivation or import and storage.

Key or CSP	Usage	Service/Access	Origin/Storage
AES symmetric encryption keys	Used to encrypt data	Encrypt: R Key Gen : W Key Wrap/Unwrap: W Key Import: W Zeroize : W	Generated or imported by the module, stored in OTP or in non-volatile Flash in plaintext
RSA public signing keys	Used to verify signatures on data	RSA Sign/Verify : R RSA Key Gen : W Zeroize : W Key Wrap/Unwrap: W Key Import: W	Generated or imported by the module, stored in volatile RAM or in non-volatile Flash in plaintext
RSA private signing keys	Used to sign data	RSA Sign/Verify : R RSA Key Gen : W Key Import: W Zeroize : W	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 : R Key Import: W RSA Key Gen : W Zeroize : W	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: R** **RSA Key Gen : W** **Key Import: W** **Zeroize : W**	**Generated or imported by the module, stored in volatile RAM or in non-volatile Flash in plaintext**
RSA public identity keys	**Used to prove identity of TPM**	**TPM Identity: R** **RSA Key Gen : W** **Key Import: W** **Zeroize : W**	**Generated or imported by the module, stored in volatile RAM or in non-volatile Flash in plaintext**
RSA private identity keys	**Used to prove identity of TPM**	**TPM Idenity : R** **RSA Key Gen : W** **Key Import: W** **Zeroize : W**	**Generated or imported by the module, stored in volatile RAM or in non-volatile Flash in plaintext**
RSA public binding keys	**Used to by an external entity to bind (wrap) a key**	**Data Binding : R** **RSA Key Gen : W** **Key Import : W** **Zeroize : W**	**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 a external entity**	**Data Binding : R** **RSA Key Gen : W** **Zeroize : W**	**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 : R** **Key Gen : W** **Key Import: W** **Zeroize : W**	**Generated or imported by the module, stored in volatile RAM or in non-volatile Flash in plaintext**

RNG seed	**Used to seed the RNG**	**Key Gen : R** **RSA Key Gen : R** **Zeroize : W**	**Generated by the module using the non-Approved non-deterministic hardware RNG (entropy source) Generated by the module, stored in volatile RAM in plaintext**
RNG Seed Key	**Used to seed the RNG**	**Key Generate : R** **RSA Key Gen : R** **Zeroize : W**	**Generated by the module using the non-Approved non-deterministic hardware RNG (entropy source), stored in volatile RAM in plaintext**
RSA Storage Root Key Private Key	**Private Root key for the hierarchy of keys associated with TPM**	**Zeroize : W**	**Generated by the module**
RSA Storage Root Key Public Key	**Public Root key for the hierarchy of keys associated with TPM**	**Zeroize : W**	**Generated by the module**
RSA Endorsement Public Key	**Used to prove to the external parties that TPM is a genuine TPM**	**TPM Endorsement : R**	**Installed at the factory**

RSA Endorsement Private Key	**Used to prove to the external parties that TPM is a genuine TPM. The key signs a challenge provided by an external party. Since the key is only known to the manufacturer, this proves to the external party that the TPM is genuine.**	**TPM Endorsement : R**	**Installed at the factory**
HMAC Authentication Key	**Used for HMAC authentication of data**	**Key Generate: W MAC/MAC Verify: R**	**Generated by the module**

Table 6. Cryptographic Keys.

Note: R is defined as read access, W is defined as write access.

6. Power-On Self Tests.

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

The module implements the following power-up cryptographic algorithm tests:

Cryptographic Function	Test Type
AES CTR encrypt	Known Answer Test (encrypt)
RSA sign/verify	Known Answer Test (sign/verify)
HMAC keyed hash	Known Answer Test (keyed hash)
RNG random number generation	Known Answer Test (generate random block)
SHS hash SHA-1	Known Answer Test (generate SHA1 digest)

Table 7. Self-tests.

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 186-3 key pair generation algorithm.

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:

a) The module must be physically controlled during the installation
b) The module must be placed on the PCB as described in the module technical specifications

9. User Guidance.

The users 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
HMAC	Hash-based Message Authentication Code
OTP	One Time programming Non-Volatile Memory
PCB	Printed Circuit Board
R	Read privilege
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir Adleman
SHS	Secure Hash Standard
SP	Special Publication
TCG	Trusted Computing Group
TPM	Trusted Platform Module
W	Write privilege

