Infineon Technologies, AG CCS TI SW

Trusted Platform Module 1.2
SLB 9660/SLB 9665/SLB 9670

FIPS 140-2 Level 1 Security Policy

Version: 1.08
Date: 25 January 2016

NON-PROPRIETARY

Table of Contents

List of Tables

List of Figures

References

Table 1: References

Acronym	Full Specification Name
[FIPS 180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, March 2012
[FIPS 186-4]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July 2013
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[FIPS197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 25 July 2013
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[SP800-56B]	NIST Special Publication SP 800-56B, Revision 1, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography,* September 2014
[SP 800-90A]	NIST Special Publication 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, January 2012
[SP800-108]	NIST Special Publication 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised),* October 2009
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[SP800-135]	NIST Special Publication 800-135, *Recommendation for Existing Application-Specific Key Derivation Function,* Revision 1, December 2011
[TPM_MP1]	TCG, *TPM Main Part 1 Design Principles*, Specification Version 1.2, Revision 116, 1 March 2011
[TPM_MP2]	TCG, *TPM Main Part 2 TPM Structures*, Specification Version 1.2, Level 2 Revision 116, 1 March 2011
[TPM_MP3]	TCG, *TPM Main Part 3 Commands*, Specification Version 1.2, Level 2 Revision 116, 1 March 2011

Acronyms and Definitions

Table 2: Acronyms and Definitions

Acronym	Definition
CCS TI SW	The Infineon group: Chip Card and Security, Technology & Innovations, Software.
CPU	Central Processing Unit
CRNGT	FIPS 140-2 AS09.42 Continuous Random Number Generator Test.
IC	Integrated Circuit
KAT	Known Answer Test
LPC	Low Pin Count interface; Intel specification for low bandwidth computing peripherals. http://www.intel.com/design/chipsets/industry/lpc.htm. An alternative to the SPI for the TPM.
MED	Memory Encrypt/Decrypt unit
MMU	Memory Management Unit
NVM	Non-Volatile Memory (e.g., EEPROM, Flash)
OSAP	Object-Specific Authorization Protocol
PCR	Platform Configuration Register
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
SPI	Serial Peripheral Interface; Motorola / de-facto standard for a synchronous serial communication interface. An alternative to the LPC for the TPM.
TCG	Trusted Computing Group (http://www.trustedcomputinggroup.org/)
TPM	Trusted Platform Module
NDRNG	True Random Number Generator (a form of hardware random number generator)

1 Overview

This document defines the Security Policy for the Infineon Trusted Platform Module 1.2 SLB 9660/SLB 9665/SLB 9670 cryptographic module, hereafter denoted *TPM*. The TPM, validated to FIPS 140-2 overall Level 1, is a single chip module that provides computer manufacturers with the core components of a subsystem used to assure authenticity, integrity and confidentiality in e-commerce and internet communications within a Trusted Computing Platform. The TPM is a complete solution implementing the TCG specifications, [TPM_MS] and [TPM_IS]. The Infineon white paper *Technology, Implementation and Application of the Trusted Computing Group Standard (TCG)*" provides a helpful introduction to TPM technology and usage. See http://www.trustedcomputinggroup.org/ for further information on TCG and TPM.

The TPM is designated as a non-modifiable operational environment under the FIPS 140-2 definitions. The FIPS 140-2 security levels for the TPM are as follows:

Table 3: Security Level of Security Requirements

Security Requirement	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	3
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	1

1.1 Versions, Configurations and Modes of Operation

Table 4: Configuration Part and Version Numbers

HW Part	Package	Firmware Version
SLB 9660	PG-TSSOP-28-2	4.80.0411.02
SLB 9665	PG-TSSOP-28-2	4.80.0411.02
SLB 9670	PG-VQFN-32-13	6.80.0113.02

The TPM is intended for use in general purpose computing environments, as a device peripheral to the CPU, with the application controlling the usage of the module. The TPM is operated in the FIPS 140-2 Approved mode when the application complies with the conditions listed in Section 8.1.

The *Show Status* service (specifically TPM_GetCapability with the CAP_VERSION_VAL qualifier) may be used to verify the FIPS-compliant version of TPM firmware is present in the TPM.

The security functions possible in the non-Approved mode are listed in Table 8.

1.2 Physical Characteristics and Cryptographic Boundary

The TPM cryptographic boundary is the surfaces, edges and connection points of the IC packages, as shown in Figure 1 (SLB 9660 or 9665 – packaging is identical) and Figure 2 (SLB 9670). The packages are shown on a 1 mm by 1 mm grid to indicate size. The physical ports and logical interfaces are detailed in Table 5.

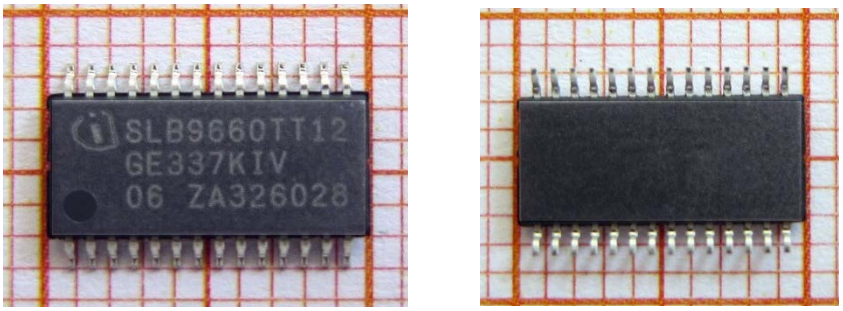

Figure 1: SLB 9660 or SLB 9665 IC package PG-TSSOP-28-2 (left: top view; right: bottom view)

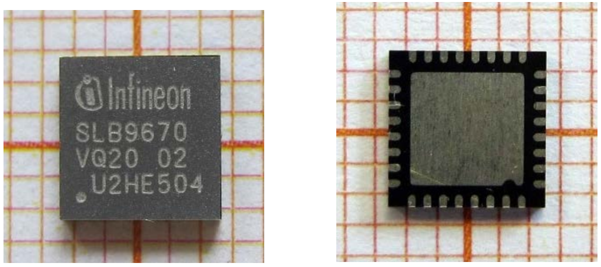

Figure 2: SLB 9670 IC package PG-VQFN-32-13 (left: top view; right: bottom view)

Table 5: Ports and Interfaces

Port	Ports common to all configurations	Logical Interface Type
GND	Ground	Power
GPIO	General Purpose I/O	Control Input, Status Output
NC	No connects	Unused
PP	Physical Presence	Control Input
VDD	3.3V	Power
LPC Interface Specific (SLB 9660 / SLB 9665) Ports and mapping to Logical Interfaces		
LAD[0:3]	Multiplexed command, address and data bus	Control Input, Data Input, Data Output, Status Output
LCLK	Clock	Control Input
LFRAME#	LPC Frame control (active low)	Control Input
LRESET#	Reset (active low)	Control Input
SERIRQ	Serial Interrupt Request	Control Input
SPI Interface Specific (SLB 9670) Ports and mapping to Logical Interfaces		
MISO	Master Input, Slave Output	Control Input, Data Output, Status Output
MOSI	Master Output, Slave Input	Control Input, Data Input, Status Output
SCLK	Serial clock	Control Input
SS	Slave Select	Control Input

1.3 TPM Logical Composition

Figure 2 depicts the TPM functional block diagram; the red outline indicates the cryptographic boundary from a logical perspective.

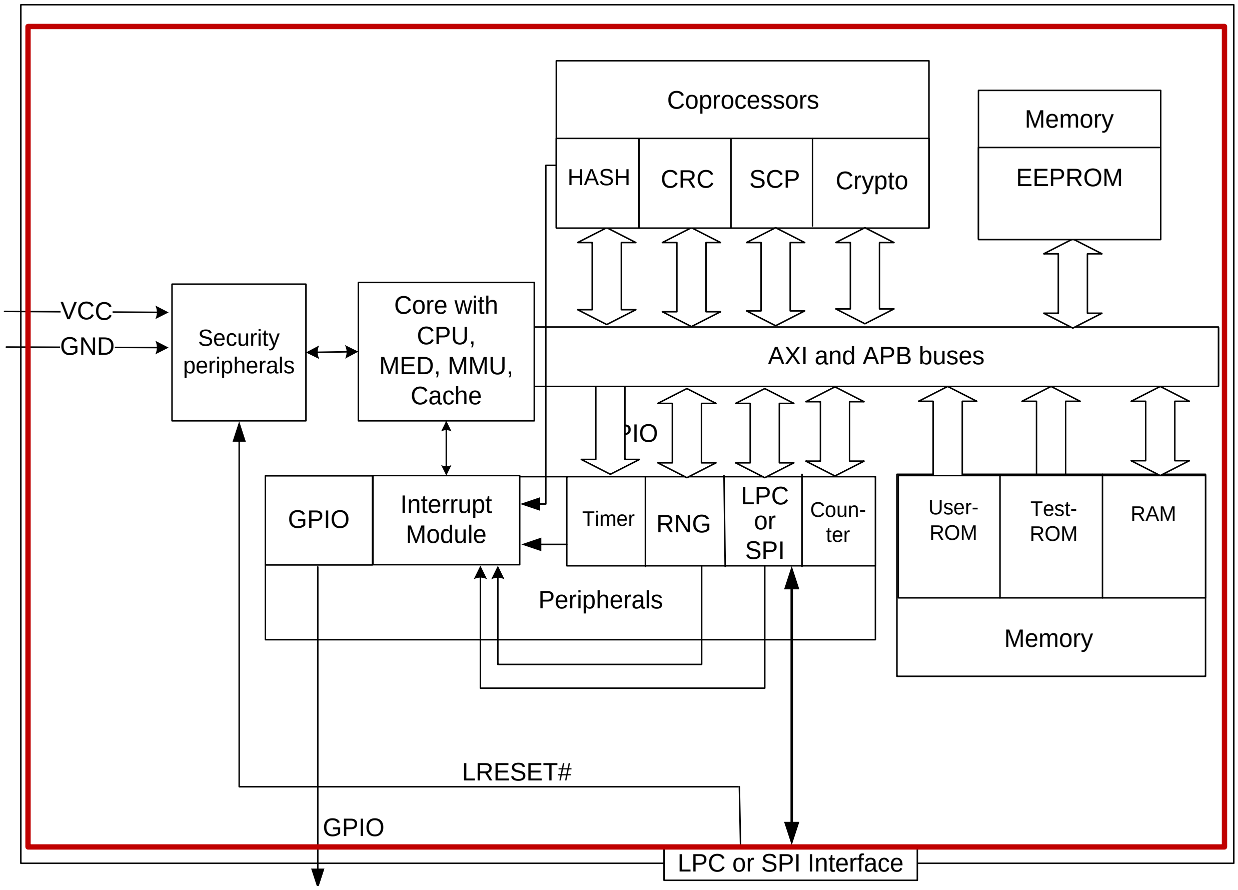

Figure 3: Module Block Diagram

The major blocks of the TPM are:

- Core: Dual CPU (configured to continuously detect faults and assure calculation integrity); MMU (memory management with privilege levels); MED (Memory Encrypt/Decrypt) and cache.
- Hardware accelerators (coprocessors): SCP (symmetric co-processor) for AES hardware acceleration; an Asymmetric Crypto Co-processor (labeled Crypto in Figure 2) for modular math (e.g. RSA 2048-bit) acceleration; a SHA-1 accelerator, labelled HASH in the figure; The checksum module allows simple calculation of 16-bit CRC checksums.
- Memory: ROM, EEPROM and RAM.
- Peripherals: timer; counter; a physical, non-deterministic random number generator called NDRNG (True Random Number Generator); and the physical ports that cross the cryptographic boundary (LPC for SLB 9660 or SLB 9665; SPI for SLB 9670).
- The LPC or SPI block corresponds to the interfaces in Table 5 above.
- Security peripherals: Security logic, shield, an interrupt-controlled I/O interface
- GPIO: Bidirectional signal which can be set or read by the caller; not otherwise used by the TPM.
- The processor firmware comprises a simple operating system with firmware that provides the TCG functionality specified in [TPM_MS]; these are the set of services described in Section 3.2.

2 Cryptographic Functionality

The TPM implements the Approved and non-Approved but allowed cryptographic functions listed in Table 6 and Table 7 below.

Table 6: Approved Cryptographic Functions

Algorithm	Description	Cert. #
AES	[FIPS 197], [SP800-38A] Advanced Encryption Standard algorithm. The module supports AES-128 encryption/decryption in CBC and CTR mode.	3523 & 3524
DRBG	[SP 800-90A] AES-128 CTR_DRBG random bit generation; uses the SP 800-90A derivation function.	882 & 883
HMAC-SHA1	[FIPS 198-1] keyed hashing using SHA-1.	2251 & 2252
KB KDF	[SP 800-108] HMAC-SHA1 key derivation function.	70 & 71
RSA	[FIPS 186-4] RSA 2048-bit key generation	1809 & 1810
RSADP	[SP 800-56B] RSADP 2048-bit key decryption primitive.	580 & 583 (CVL)
RSAEP	[SP 800-56B] RSADP 2048-bit key encryption primitive. Not testable through CAVP. Vendor-affirmed per IG D.4.	N/A
RSASP1	[FIPS 186-4 RSA; PKCS#1v2.1] RSASP1 signature primitive (RSA 2048-bit key).	581 & 584 (CVL)
SHA-1	[FIPS 180-4] Secure Hash Standard compliant one-way (hash).	2905 & 2906
TPM KDF	[TPM SP 800-135] Section (TPM) key derivation function. The following statement is required by IG D.11: The TPM protocol has not been reviewed or tested by the CAVP or CMVP.	579 & 582 (CVL)
Symmetric key wrap	Symmetric key encryption using AES-128 for encryption and decryption with HMAC-SHA-1 used for integrity; allowed per IG D.9. Provides 128 bits of strength.	AES & HMAC certs. (see above)

Table 7: Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
NDRNG	True Random Number Generator (hardware RNG classified as NDRNG in the AIS 31 scheme); minimum of 8-bit per access. The NDRNG output is used only to seed or reseed the FIPS approved DRBG.
Asymmetric key encapsulation/ decapsulation	RSA 2048-bit key encapsulation and decapsulation. Provides 112 bits of strength.

Table 8: Non-Approved Cryptographic Functions possible in the non-Approved mode

Algorithm	Description
RSA	RSA 1024-bit key generation, signature generation and signature verification.
RSADP	1024-bit key decryption primitive.
SHA-1	Use of SHA-1 for RSA signature generation.

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section.

RSA Key Encapsulation / Decapsulation (using the RSAEP and RSADP primitives) protects keys provided by the TPM to the calling application. RSA 2048 keys are used exclusively for this purpose, providing 112 bits of security for the key encapsulation process.

Table 9: Cryptographic Keys and CSPs

CSP	Description/Usage
DRBG-EI	256 bits of entropy input produced by the NDRNG, used during DRBG instantiation and reseed.
DRBG-STATE	Current values of DRBG state (V and K). 128 bit each.
TPM-EK	TPM Endorsement Key - RSA 2048 bit private key uniquely associated with each TPM device over the TPM life time. The Endorsement Key pair is installed at the factory, is used to establish that the TPM is authentic, and as such, cannot be destroyed.
TPM-SRK	TPM Storage Root Key - RSA 2048 bit private key used to decapsulate SK instances.
TPM-SK	TPM Storage Key - RSA 2048 bit private key used to decapsulate other keys in the Protected Storage hierarchy.
TPM-SEAL	TPM Seal Key - RSA 2048 bit private key used to seal and unseal arbitrary data.
TPM-AIK	TPM Attestation Identity Key - RSA 2048 bit private key used for signature generation for TPM reporting.
TPM-USK	TPM User Signing Key - RSA 2048 bit private key used for signature generation.
TPM-UBK	TPM User Binding Key - RSA 2048 bit private key used for decryption of user keys.
TPM-SMAC	Ephemeral HMAC-SHA1 160 bit key used for message authentication in TPM authorization protocols.
TPM-IPK	TPM Integrity Protection Key - HMAC-SHA1 160 bit key used for integrity protection of encrypted data.
TPM-MK	TPM Master Key (Key Derivation symmetric key) - HMAC-SHA1 160 bit key Used to derive ephemeral confidentiality protection symmetric keys.
TPM-EDK	Ephemeral AES 128 bit key used to: 1) encrypt authentication information and 2) provide confidentiality for TPM command data transmission.
TPM-KEK	Ephemeral Key Encryption Key - AES 128 bit key used to protect CSP confidentiality.

2.2 Public Keys

Table 10: Public Keys

Key	Description/Usage
TPM-PUBEK	TPM Public Endorsement Key - RSA 2048-bit public key uniquely associated with each TPM device over the TPM life time.
TPM-PUBSRK	TPM Public Protected Storage Root Key - RSA 2048-bit public key used to encapsulate SK instances.
TPM-PUBSK	TPM Public Storage Key - RSA 2048-bit public key used to encapsulate other keys in the Protected Storage hierarchy.
TPM-PUBSEAL	TPM Public Seal Key - RSA 2048-bit public key used to seal and unseal arbitrary data.
TPM-PUBAIK	TPM Public Attestation Identity Key - RSA 2048-bit public key used for signature verification for TPM reporting.
TPM-PUBUSK	TPM Public User Signing Key - RSA 2048-bit public key used for signature verification
TPM-PUBUBK	TPM Public User Binding Key - RSA 2048-bit public key used for encryption of user keys.

3 Roles, Authentication and Services

The TPM supports two roles, a CO role and a User role, as described in Table 11. Although authentication is not required for FIPS 140-2 Level 1, the CO and User roles are authenticated as described in Section 3.1.

The TPM:

- Does not support a maintenance role or concurrent operators.
- Requires re-authentication following a power cycle

Table 11: Roles Supported by the Module

Role ID	Role Description
CO	Cryptographic Officer, also known as the TPM owner. Performs cryptographic initialization (e.g., creation of Storage Root Key) and management functions.
User	User, also known as the entity owner. Uses the TPM to create a cryptographic entity and obtain cryptographic services for that cryptographic entity.

3.1 TPM Identification and Authentication Method

Although the module is Level 1, it does provide operator authentication. Although not formally required, this section describes the authentication provided by the module. Described as *data authorization* by the TCG specification, operators in the CO or User roles are authenticated by a challenge and response demonstration of knowledge of a shared secret (the TPM identification and authentication data). Both the TPM ownership token and entity token (the CO and User authentication data, respectively) are HMAC-SHA-1 keys. The TPM data authorization mechanism includes nonce values to prevent replay attacks.

The probability that a random attempt will succeed using this authentication method is:

- $2^{-160} = 6.8\times10^{-49}$

A very conservative estimate of the maximum authentication rate is 10^6 / minute (60 µs per attempt). The probability that a random attempt will succeed over a one-minute interval based on this rate and the probability of false authentication established above is:

- $10^{6} \times 6.8\times10^{-49} = 6.8\times10^{-43}$

3.2 Services

All services implemented by the TPM are listed in the tables below, with corresponding access to CSPs. See [TPM_MP3] for a public description of all commands. The following codes are used for CSP access in these tables:

- G = Generate: The TPM generates the CSP.
- R = Read: The TPM reads the CSP (a CSP is output by the TPM).
- E = Execute: The TPM executes using the CSP.
- W = Write: The TPM writes or updates the CSP; generation and zeroization are special cases.
- Z = Zeroize: The module zeroizes the CSP.
- -- = Not accessed by the service.

Table 12: Unauthenticated TPM Services

Unauthenticated Services	DRBG-EI	DRBG-STATE	TPM-EK	TPM-SRK	TPM-SK	TPM-SEAL	TPM-AIK	TPM-USK	TPM-UBK	TPM-SMAC	TPM-IPK	TPM-MK	TPM-EDK	TPM-KEK
DRBG Services: Generate random bits		E												
Generate hash (extend PCR)	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Manage PCR security attributes	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Reset / Power-cycle (entropy input destroyed after use)	GEZ	GZ	--	--	--	--	--	--	--	--	--	--	--	--
Zeroization (requires Physical Presence signal assertion)	Z	Z	--	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z

Table 13: CO Authenticated TPM Services

CO Services	DRBG-EI	DRBG-STATE	TPM-EK	TPM-SRK	TPM-SK	TPM-SEAL	TPM-AIK	TPM-USK	TPM-UBK	TPM-SMAC	TPM-IPK	TPM-MK	TPM-EDK	TPM-KEK
Derive keys: - SP 800-135 TPM KDF - SP 800-108 KDF	--	--	--	--	--	--	--	--	--	G	--	E	G	G
Generate RSA key pair	--	EW	--	G	--	--	G	--	--	--	--	--	--	--
Generate symmetric key (AES, HMAC)	--	EW	--	--	--	--	--	--	--	--	--	--	--	--
HMAC generate and verify	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Initialize	--	--	E	--	--	--	--	--	--	--	--	--	--	--
Manage TPM operational modes (Requires Physical Presence signal assertion)	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Read public key	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Self-test	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Show status	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Symmetric encryption/decryption: - Encrypt authentication protocol data - Transport Session confidentiality - Session closure destroys session keys	--	--	--	--	--	--	--	--	--	Z	--	--	EZ	EZ
Zeroize (key destruction via memory overwrite)	Z	Z	--	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z

Table 14: User Authenticated TPM Services

User Services	DRBG-EI	DRBG-STATE	TPM-EK	TPM-SRK	TPM-SK	TPM-SEAL	TPM-AIK	TPM-USK	TPM-UBK	TPM-SMAC	TPM-IPK	TPM-MK	TPM-EDK	TPM-KEK
Derive keys: - SP 800-135 TPM KDF - SP 800-108 KDF	--	--	--	--	--	--	--	--	--	G	--	E	G	G
DRBG Services - Generate random bits - Reseed	--	ER	--	--	--	--	--	--	--	--	--	--	--	--
Encrypted key entry and output - RSA key encapsulation - Symmetric key wrapping (AES)	--	--	--	E	E R W	E R W	R W	R W	R W	--	--	--	--	E
Generate RSA key pair	--	--	--	--	G	G	--	G	G	--	--	--	--	--
Generate symmetric key (AES, HMAC)	--	--	--	--	--	--	--	--	--	--	G	G	G	G
HMAC generate and verify	--	--	--	--	--	--	--	--	--	E	E	--	--	--
Manage TPM operational modes (Requires Physical Presence signal assertion)	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Read public key	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Self-test	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Show status	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Sign (hash performed off-module)	--	--	--	--	--	--	--	E	--	--	--	--	--	--
Store or get data (with authorization)	--	--	--	--	--	E	--	--	E	--	--	--	--	--
Symmetric encryption/decryption: - Encrypt authentication protocol data - Transport Session confidentiality	--	--	--	--	--	--	--	--	--	--	--	--	E	E

4 Self-test

On power-on or reset, the TPM performs self-tests as described in Table 15 below. All KATs must be completed successfully prior to any other use of cryptography by the TPM. If one of the KATs fails, the system is halted (in the Failure Mode state). In this mode only TPM_GetTestResult is accepted by TPM to self-test error status; no CSP access is possible. Self-tests may be invoked at any time using TPM_SelfTestFull, with self-test results returned using TPM_GetTestResult.

Table 15: TPM Self-Tests

Critical Function Self-Tests	
Hardware Integrity Test	The TPM performs a hardware integrity test at power-up and at fixed periods. In either case, if the hardware integrity tests fails, TPM hardware immediately enters a security reset state (the TPM is mute).
Power-On Self-Tests	
Firmware Integrity	SHA-1 message digest performed over all code located in NVM. This integrity test is not required or performed for code stored in masked ROM code memory.
DRBG KATs (Cert. #882 & 883)	Performs a fixed input KAT, inclusive of the SP 800-90A health monitoring tests.
AES KATs (Cert. #3523 & 3524)	Performs separate encrypt and decrypt KATs using an AES-128 key in CBC mode.
RSA KATs (Cert. #580 & 583, #581 & 584)	Performs RSASP1/RSADP and RSAEP KATs using an RSA 2048-bit key.
SHA-1 KAT (Cert. #2905 & 2906)	Performs a fixed input KAT using SHA-1.
HMAC-SHA-1 KAT (Cert. #2251 & 2252)	Performs a fixed input KAT using HMAC-SHA-1.
KBKDF (Cert. #70 & 71)	Performs a fixed input KAT of the SP 800-108 KDF.
TPM KDF(Cert. #579 & 582)	Performs a fixed input KAT of the SP 800-135 TPM KDF.
Conditional Self-Tests	
RSA Key Gen PCT	On generation of each RSA key pair, the TPM performs a pairwise consistency test using the RSA primitive operations. For key transport keys, the PCT sequence is encrypt/decrypt; for signature keys, the PCT sequence is sign/verify.
DRBG CRNGT	The TPM performs the AS09.42 CRNGT to assure the DRBG output is different than the previous value. Failure of this DRBG CRNGT is handled as an attack; the TPM enters an error state.
NDRNG CRNGT	The TPM performs the AS09.42 CRNGT at the hardware level to assure the DRBG output is different than the previous value. Failure of this NDRNG CRNGT is treated as an attack; the TPM enters an error state.

5 Physical Security Policy

The TPM is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The TPM employs standard passivation techniques. The TPM is intended for deployment on standard PCBs or similar assemblies.

6 Electromagnetic Interference and Compatibility (EMI/EMC)

The Module conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

7 Mitigation of Other Attacks Policy

The TPM implements the mechanisms listed in Table 16 to mitigate attacks beyond the requirements of FIPS 140-2 Security Level 1. There are no specific limitations for any of these attack mitigations.

Table 16: Mitigation of Other Attacks

Other Attack	Mitigation Mechanism
Fault induction	External clock conditions, temperature and electromagnetic radiation (e.g. light) are monitored using sensors. Operation outside specific parameters causes the chip to enter the *Security reset* state until the condition is cleared.
Software fault induction	The virtual physical address mapping together with the memory management unit (MMU) gives the possibility to define different access rights for memory areas. In case of an access violation (e.g., embedded software trying to read memory of IC-dedicated software) hardware enters the *Security reset* state.
EEPROM memory corruption	The memory system maintains EEPROM data integrity using an error detection and correction mechanism at the hardware level. A 1-bit (per byte) error is automatically corrected; multiple-bit errors a cause the TPM to enter the *Security reset* state.
Design analysis and surveillance attacks (in operational or power off conditions)	The TPM integrated circuit level layout uses masking, critical circuit shielding and synthesized logic to deter attacker knowledge of the part design. Outer layer lines are protected with a proprietary masking technique, with active shielding in internal layers to protect the masking mechanism. The use of synthesized logic deters attackers from pattern recognition of logic clusters. As well, a dedicated CPU with a non-public bus protocol is used which makes analysis complicated.
Physical probing of memory and data buses.	Proprietary memory and bus masking to deter probing memories or buses.

8 Security Rules and Guidance

The TPM implementation also enforces the following security rules:

- No additional interface or service is implemented by the Module which would provide access to CSPs.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
- The module does not support manual key entry.
- The module does not output plaintext CSPs or intermediate key values.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

8.1 Requirements for Secure Operation

The application must assure the following conditions are met for operation of the TPM in the FIPS 140-2 Approved mode:

- Only Approved and allowed cryptographic functions shall be used. Refer to the list of corresponding cryptographic functions in Tables 12, 13 and 14.
- The TPM_OSAP authentication protocol with TPM_ET_AES128_CTR shall be used for authentication.
- Only RSA keys having modulus size 2048 bit shall be used in cryptographic operations.
- SHA-1 hash values generated by TPM shall not be used for subsequent signature generation.
- RSA-2048 signature generation with SHA-1 as a hash function shall not be used for TPM Sign; all other potential uses of non-Approved RSA are covered by the disallowed commands listed next.
- The following commands that do not meet the above criteria or use non-Approved cryptographic functions shall not be used in the FIPS 140-2 Approved mode of operation:
  - TPM_DAA_Join
  - TPM_DAA_Sign
  - TPM_CertifyKey
  - TPM_CertifyKey2
  - TPM_MakeIdentity
  - TPM_Quote
  - TPM_Quote2
  - TPM_ReleaseTransportSigned
  - TPM_TickStampBlob
  - TPM_MakeIdentity