Microchip Technology Inc

Microchip Trust Anchor TA100
FIPS 140-2 Non-Proprietary Security Policy

Document Version: 3.0

HW Part Numbers	HW Revision	FW Revision		
		CP ROM	ACE ROM	DevUpdate
TA100-Y230C2X01	59V01B5	0x0006	0x04	0x00B50002
TA100T-Y230C2X01				
TA100-Y240C2X01	59V01B6	0x0007	0x04	0x00B60001
TA100T-Y240C2X01				
TA100-Y240D3X01				
TA100-Y240UFB01				

September 09, 2022

REVISION HISTORY

Ver	Date	Author(s)	Updates
3.0	09/09/2022	Jim Hallman	Initial Public Release

Table of Contents

1. Introduction

Microchip Trust Anchor TA100 Cryptographic Module is a single chip cryptographic module. The Microchip Trust Anchor Security Device (may also be referred to as the module or TA100) is intended for automotive, industrial or commercial systems and can provide support for code authentication (aka secure boot), message MAC generation, support for trusted firmware updates, building blocks for multiple key management protocols including TLS and other root-of-trust based operations. It is typically a companion device to an MCU or MPU on the same board.

The TA100 securely stores keys for SHA-256, HMAC, CMAC, RSA, ECDSA, and ECDH among other algorithms. The chip can use these keys to sign challenges and return a MAC or signature that proves it knows the secret key or that it owns the private key associated with an RSA or ECC public key. The TA100 also implements AES-GCM, AES-CMAC and SHA-HMAC encryption and AES-GCM and AES-ECB decryption.

The Microchip TA100 hardware and corresponding firmware revisions of the product that are certified to this security policy are listing in Table 4-2

2. Security Level Specification

The following table lists the level of validation for each area in the FIPS PUB 140-2.

SECURITY REQUIREMENTS AREA	LEVEL
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	3 (With EFP)
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Table 2-1 – Security Level Table.

3. Cryptographic Boundary

The following diagram defines the cryptographic boundary, which is the perimeter of the single-chip module.

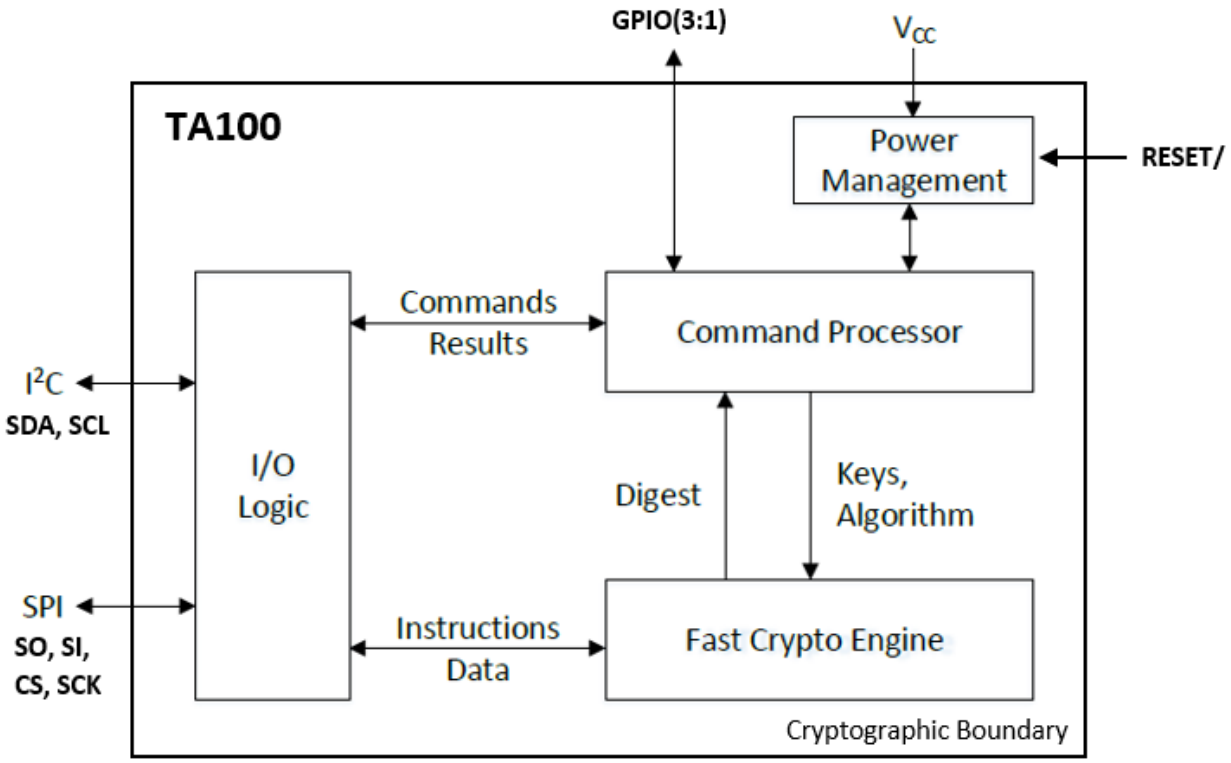

Figure 3-1 – The Cryptographic Boundary of the *Microchip Trust Anchor TA100*

4. Physical Ports and Logical Interfaces

The Cryptographic Module provides the following physical ports and interfaces.

	Physical Port					
Die Pad	**8-pin SOIC SPI**	**8-pin SOIC I2C**	**14-pin SOIC SPI & I2C**	**24-pin VQFN SPI & I2C**	**Logical Interface**	**Function**
GPIO_1	-	X	X	X	Data Input Data Output Status Output	General purpose IO pin
GPIO_2	-	X	X	X	Data Input Data Output Status Output	General purpose IO pin
GPIO_3	X	X	X	X	Data Input Data Output Control Input Status Output	General purpose IO pin
SDA	-	X	X	X	Data Input Data Output Control Input Status Output	I^2C Data
SCL	-	X	X	X	Control Input	I^2C Clock
CS/	X	-	X	X	Control Input	SPI Chip select
SI	X	-	X	X	Data Input Control Input	SPI Serial data input
SCK	X	-	X	X	Control Input	SPI clock
SO	X	-	X	X	Data Output Status Output	SPI Serial data output
RESET/	-	X	X	X	Control Input	Reset Input, active low
RESET2/	X	-	-	-	Control Input	Alternate Reset Input, active low
Vss	X	X	X	X	Power	Ground
Vcc	X	X	X	X	Power	2.7 – 5.5V Power Supply

Table 4-1 - Specification of Cryptographic Module Physical Ports and Logical Interfaces

4.1. Unit Identification

The TA100 is manufactured in four package configurations. The TA100 Hardware and Firmware versions implemented in the FIPS evaluated and certified versions of the device are listed in Table 4-2:

HW Part Number	Package / Interface	HW Revision	FW Revision		
			CP ROM	ACE ROM	DevUpdate
TA100-Y230C2X01	SOIC-8 SPI	59V01B5	0x0006	0x04	0x00B50002
TA100T-Y230C2X01	SOIC-8 I2C				
TA100-Y240C2X01	SOIC-8 SPI	59V01B6	0x0007	0x04	0x00B60001
TA100T-Y240C2X01	SOIC-8 I2C				
TA100-Y240D3X01	SOIC-14 SPI & I2C				
TA100-Y240UFB01	VQFN-24 SPI & I2C				

Table 4-2 – Device Configurations

Device marking does not identify the TA100 certified product number. However, the user can easily confirm the revision of the product by executing the INFO command. The following two executions of the INFO command will provide the full detail of the device revision information. The below example is specific to 59V01B6 devices. Comparable information is reported for 59V01B5 devices.

INFO with Mode byte set to 0x00

This will return the revision of the internal hardware and ROM codes of the device. The output data from the command will be comparable to the below byte string:

0x00 0x0D 0x00 **0x00 0x02 0x00 0x07** 0xXX 0xXX **0x04** 0xXX 0xXX 0xXX

Hardware revision 59V01B6: Byte 0,1	0x0002	(59V01B5 value: 0x0001)
CP ROM revision: Byte 2,3	0x0007	(59V01B5 value: 0x0006)
ACE ROM revision: Byte 6	0x04	(59V01B5 value: 0x04)

INFO with Mode byte set to 0x07

This will return the revision of the DevUpdate Code. The output data from the command will be comparable to the below:

0x00 0x15 0x00 0xXX 0xXX 0xXX 0xXX 0xXX 0xXX 0xXX 0xXX 0xXX **0xB6 0x00 0x01 0x00** 0xXX 0xXX 0xXX 0xXX

DevUpdate Code revision	0xB6 0x00 0x01 0x00 equates to 0x00B60001
	0xB5 0x00 0x02 0x00 equates to 0x00B50002

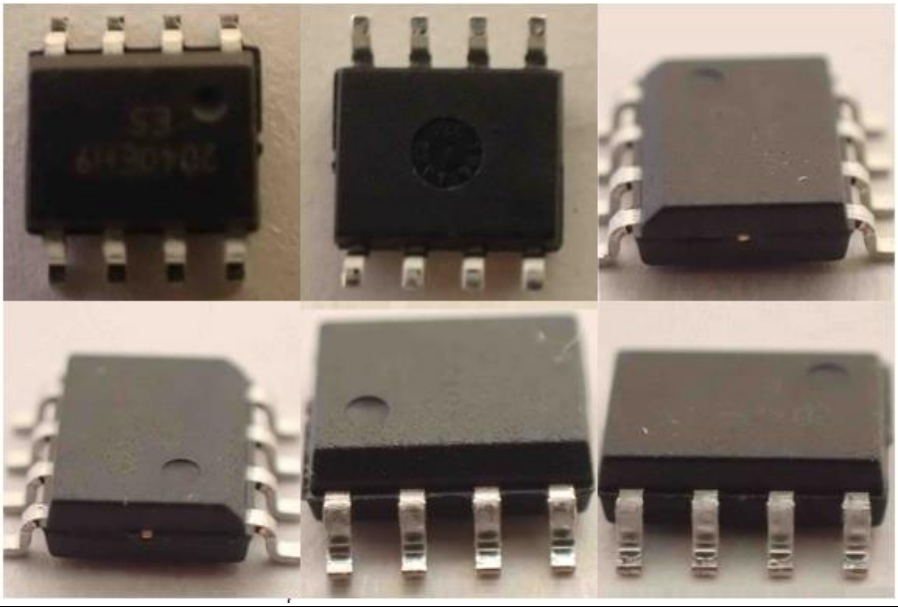

Figure 4-1 – 8-SOIC TA100-Y230C2X01 or TA100-Y240C2X01

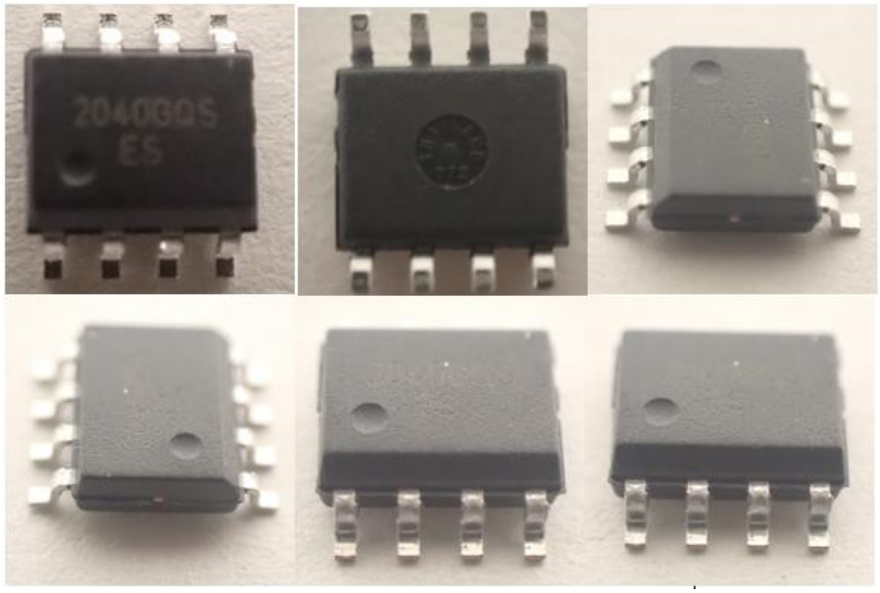

Figure 4-2 – 8-SOIC TA100T-Y230C2X01 or TA100T-Y240C2X01

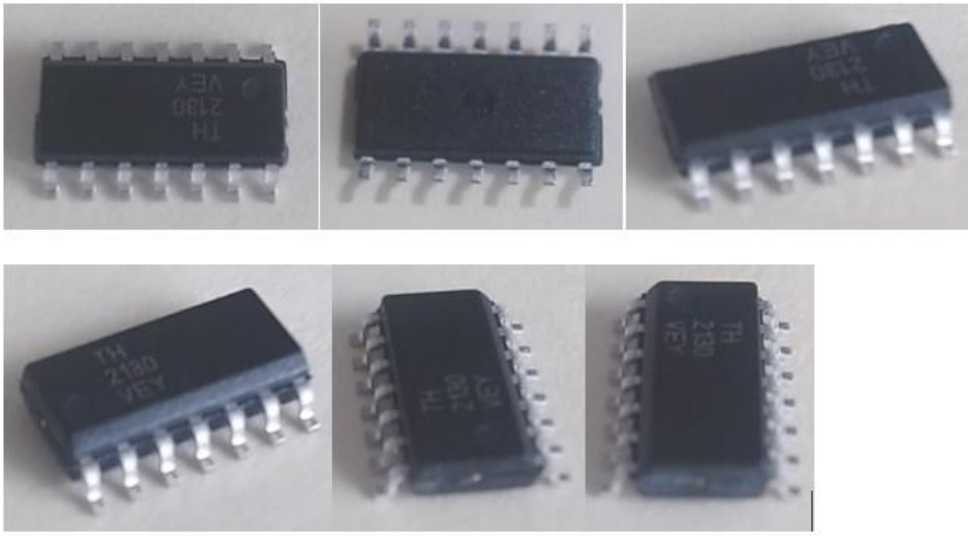

Figure 4-3 – 14-SOIC TA100-Y240D3X01

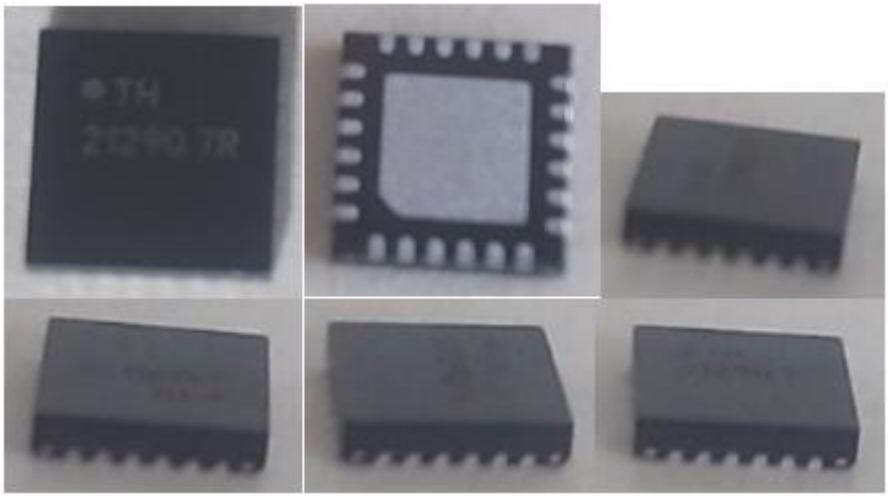

Figure 4-4 – 24-VQFN TA100-Y240UFB01

5. Modes of Operation and Security Rules

5.1. Modes of Operation

The module has a Compliance mode of operation which is detailed in this security policy. Operating the module in this mode means that the module is running in the FIPS 140-2 Approved Mode of Operation.

If Compliance mode is desired the operator shall,

- Configure the module to run in FIPS Mode as specified in section 5.2.
- Execute all required self-tests and ensure that they have passed.
- Follow all applicable security rules in section 5.3.

If the above conditions are not met the module is considered to be running in non-Complaint mode (non-Approved Mode of Operation).

5.2. Compliance Mode Configuration

There is only one combination of configuration bits that allow the device to be in the FIPS compliant mode of operation. These configuration bits are detailed below. Other configuration bits within the device have no impact on the Compliance Mode (FIPS mode) of operation and are not detailed here. See the product datasheet for further details about these configuration bits.

Once the device configuration is locked and the product is in the Compliance Mode, the device configuration cannot be modified for the life of the device.

To invoke the FIPS mode of operation the module must be configured with the following:
Minimum Compliance configuration:

1. Set self_test_config.Power_Up = 0x7F3A 0200
2. Set self_test_config.Wake = 0xXXXX XXXX
3. Set self_test_config.On_Demand = 0xXXXX XXXX
4. Set self_test_config.Failure_Clear = 0x7F3A 0200
5. The operator must set the Failure_Clear map to be the same as the Power_Up map. This will ensure that if a self-test fails the module will not clear the error flag until all of the required FIPS algorithms pass their self-tests.

Firmware Update configuration:

1. Set Device_Update.Power_up_check = 0x1
2. Set Device_Update.Auth_Update = 0x1
3. Set Device_Update.Update_Key = KKK (KKK=ID of Key)

All other bits may be configured at the discretion of the user.

Device_Update.Downgrade_OK and Device_Update.Erase_OK are strongly recommended to be set to 0x0.

Master delete configuration:

1. Set chip_option.Compliance = 0x1
2. Set Master_Delete.Enable = 0x1
3. Set Master_Delete.Auth_Key = KKK (KKK=ID of Key)

Chip Options configuration:

1. Set chip_option.Reset_Fail=0x0
2. Set chip_option.ECDB=0x1
3. Set chip_option.Sign_Internal_Auth = 0x1

All other bits may be configured at the discretion of the user.

Compliance configuration:

1. Set compliance_option.Chip_Erase = 0x1
2. Set compliance_option.Config_Test = 0x1
3. Set compliance_option.Update_Test = 0x1
4. Set compliance_option.Public_Auth = 0x1
5. Set compliance_option.RW_SHA_CTX = 0x0

All other bits may be configured at the discretion of the user.

Secure Boot Configuration:

1. Mode = 2, Full Stored, is not permitted

Global Export configuration:

2. Set Global_Export.Forbid = 0x0
3. Set Global_Export.Auth_Req = 0x1
4. Set Global_Export.Auth_Key = KKK (KKK=ID of Key)

Alternate configurations are permitted as long as the combination Global_Export.Forbid ==0 AND Global_Export.Auth_Req == 0 is never configured.

5.3. Self-Test Failure and Recovery

Upon encountering a self-test failure, the TA100 will remain in self-test failure state until an error recovery is attempted. While the module is in an error state, data output (except for status data) is inhibited by the module. The module will not allow any operations or commands other than Run Self-tests (Cryptographic Self-Test service), Show Status (Device Information and Status service), and Power Management to be executed.

To recover the module the operator must re-run the self-tests successfully without any failures.

If the operator successfully re-ran self-test and all of the required self-tests passed, the device will exit the error state and allow normal operation. The operator may execute the show status command to check if the model is ready to receive commands.

5.4. Security Rules

The following specifies the security rules under which the cryptographic module shall operate:

- When configuring the module, the Personalization[1] option shall not be used.
- The COK must always be generated in the range of 80F0 – 80FF
- The Transport Key shall only be used to enter the COK T=0 key.
- Public keys shall not be entered or output in plaintext. These keys shall only be entered or output using AES GCM ASK.
- Private keys that are outside of the module's boundary shall not be used to regenerate public keys.
- When performing the Device Update service, the operator shall
    - Authenticate as the CO.
    - Ensure that the Power_up_check bit is set.
- Certificate revocation shall not be used in FIPS mode of operation.
- Key Generation shall only be performed inside an Authorization Session.
- The ECDH command shall only be performed inside an Authorization Session.
- The ECDH command mode bit 3 shall be set.
- Exporting public keys using AES GCM ASK shall only be performed inside an Auth Session.
- The Master Delete function shall only be used in an Authorization Session.
- RSA and ECC keys shall only be generated using SP800-90A DRBG (using SP800-56A is disallowed).
- The module supports a maximum of simultaneous 2 Auth Sessions (i.e. a maximum of two concurrent operators).
- TLS 1.3 HKDF shall not be used.
- The cryptographic module does not provide any service/interface to output authentication data in plaintext. With the exception of the initialization procedures that allow for manual transport and electronic entry of plaintext secret keys (that will require human operators physically present at the cryptographic boundary and procedural guidance's) the cryptographic module does not support plaintext CSP entry. Once the cryptographic module has been initialized, all subsequent services/operations that allow for modifications and outputs of CSPs occur over a mutually authenticated and encrypted Authorization session.

- The module does not output the GCM keys or any information that could be used to determine the GCM keys during the initialization procedures and during all operations where the GCM keys are being used.
- The IV is generated using an Approved DRBG using a 96-bit seed generated inside the module's physical boundary.
- The IV is always regenerated after power is lost.
- Optionally in 59V01B6 based devices, the user may configure the module to support an external tamper response service through a control input where user identified keys will be deleted when a low level is detected, followed by a device reset.

Note[1]: The Personalization option is a process used to write the update master keys using a fixed transport key which cannot be zeroized.

6. Cryptographic Algorithms

6.1. Approved Algorithms

The following table shows all algorithms with the associated CAVP certificates for the different implementations validated in the module.

CAVP CERT. #	ALGORITHM	STANDARD	MODE/METHOD	KEY LENGTHS, CURVES, OR MODULI	USE
A855	AES ECB	FIPS 197	ECB encrypt only	128	FCE AES128-ECB Encrypt
A874	AES CMAC	SP800-38B	Generate	128	FCE AES128-CMAC Generate
A854	SHA	FIPS 180-4	SHA-256		FCE SHA2-256
A853	HMAC	FIPS 186-1	w/ SHA2-256	256	FCE SHA256-HMAC Keyed Hash
A851	AES ECB	FIPS 197	ECB encrypt/decrypt	128	ACE AES128-ECB Encrypt / decrypt
A2515	AES CTR	FIPS 197	Internal Counter mode	128	ACE AES128 internal counter mode
A852	AES CMAC	SP800-38B	generate/verify	128	ACE AES128-CMAC Generate / Verify
A851	AES GCM GMAC	SP800-38D	encrypt/decrypt	128	ACE AES128-CMAC Generate / Verify
A856	SHA	FIPS 180-4	SHA-256		ACE SHA2-256
A859	HMAC	FIPS 186-1	w/ SHA2-256	256, 384	ACE HMAC-SHA2-256 Keyed Hash
A850	DRBG	SP800-90A	CTR_DRBG w/ derivation function	AES-128	Random bit Generation
A860	ECDSA[1]	FIPS 186-4		P224, P256, P384 KeyGen, SigGen, SigVer	Digital Signature Provides between 112 and 192 bit security strength
A1021, A1022 and A1023	KAS[1,2]	SP800-56Ar3	Ephemeral Unified C(2e, 0s, ECC CDH) scheme	P224, P256, P384	Provides between 112 and 192 bit security strength
	ENT (P)	SP 800-90B			Used as entropy source for seeding SP800-90A DRBG.

CAVP CERT. #	ALGORITHM	STANDARD	MODE/METHOD	KEY LENGTHS, CURVES, OR MODULI	USE
					Provides 128 bits of entropy.
A875	RSA	FIPS 186-4	PKCSv15 and PSS SHA2-256	2048 KeyGen, SigGen, SigVer	Digital Signature 112-bit security strength
A875	RSA	FIPS 186-4	PKCSv15 and PSS SHA2-256	3072 Verify	Digital Signature 128-bit security strength
A858	KBKDF	SP800-108	HMAC-Counter w/ SHA2-256		Key Derivation
A857	KDF TLS 1.2[3,4]	SP800-135			Key Derivation
Vendor Affirmed	CKG	S800-133r2			[SP 800-133r2, Section 5] Seeding for asymmetric key generation uses unmodified DRBG output [SP 800-133r2, Section 6.1] Symmetric key generation uses unmodified DRBG output

Table 6-1 – Table of Approved Algorithms

Note[1]: Entropy Caveat - The module generates cryptographic keys whose strengths are modified by available entropy.
Note[2]: IG D.8 scenario X1, path (2)
Note[3]: KDF certificates are CVLs.
Note[4]: As per IG D.11, no parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.

6.2. Non-Approved but Allowed Algorithms

The following table describes the non-approved cryptographic but allowed algorithms supported by the Cryptographic Module in Approved mode.

ALGORITHM	USE (no security claimed)
LFSR (Non-FIPS)	Used for obfuscation within the crypto engine, dummy cycles, randomization for attack resistance
Masking / Blinding	obfuscation
Persistent Storage Obfuscator NVM	Used for obfuscation of data stored in NVM
Persistent Storage Obfuscator ROM	Used for obfuscation of data stored in ROM
RSA[2]	2048 Encrypt/Decrypt
Transport Pre-Key	Used for obfuscation of Master DevUpdate Key (MDUK), DevUpdate Public Key (DUPK) entry
Transport Key	Used to obfuscate manual entry during FIPS initialization
Transient Storage Obfuscator	Used for obfuscation of data stored in SRAM
Utility RNG	Used for NVM wear leveling or various obfuscation purposes

Table 6-2 – Table of Non-Approved but Allowed Algorithms

Note[2]: Per IG 1.23, no security is claimed for the non-approved RSA encrypt/decrypt allowed in FIPS mode because it is not security relevant, and it is used over a protected and authenticated channel.

6.3. Non-Approved Algorithms

The following table describes the non-approved cryptographic algorithms supported by the Cryptographic Module in non-Approved mode.

ALGORITHM	USE
KDF AES Option A	HDCP
KDF AES Option B	HCDP
ECBD	group key agreement
KDF SHA	Used for ECBD flow
KDF HKDF	Used for TLS 1.3
ECDSA SECP256K1	Bit Chain applications
ECDSA Brainpool-256	Used for non-compliant signatures
ECDH Brainpool-256	Used for non-compliant key agreement

Table 6-3 – Table of Non-Approved Algorithms

7. Services and Access Control Policy

The list below describes the roles, services, cryptographic keys & CSPs, and types of access to the cryptographic keys & CSPs that are available to each of the authorized roles via the corresponding services.

#	Service	No Auth	User (Auth)	CO (Auth)	Description	Keys and CSPS/ Type(s) of Access R=read, W=write, E=execute, Z=zeroize
1	Device Information and Status	X	X	X	This service provides device information and state.	N/A
2	Power Management	X	X	X	This service manages the operating mode of the device relative to power.	CTR KEK (Z) Proof Key (Z) DevUpdate Key (Z)
3	Device Configuration	X	X	X	This service sets the configured capabilities of the device. This service creates the FIPS device.	N/A
4	Auth Session[1] (Auth)		X	X	This service sets up an auth session to limit user service access.	UAK (E) ASK (W, Z) COK T=0 (E) COK2 (E) PSK (W, Z) UAK (E) ASK (W, Z)
5	Data Element Creation	X	X	X	This service creates non-CSP elements in the shared data memory or a volatile register with specific attributes.	N/A
6	CSP Element Creation		X	X	This service creates CSP elements (private and public, symmetric, and	Auth[2] (E) ECDH Shared secret Z (E, W, Z) SP800-56C Salt (E, W, Z)

#	Service	No Auth	User (Auth)	CO (Auth)	Description	Keys and CSPS/ Type(s) of Access R=read, W=write, E=execute, Z=zeroize
					asymmetric) in the shared data memory or a volatile register with specific attributes.	KDK (E, W, Z) Derived Key Material (W) SP800-56C KDF Internal State (E, W, Z) SP800-108 KDF Internal State (E, W, Z) PUB_ES_Root (W) PUB_TOPKG_ECC (R) PUB_TOPKG_ECDH (R) PUB_TOPKG_RSA (R) Encrypted Storage[2] (E) Customer Keys (E)
7	Message Authentication (MAC)		X	X	This service authenticates incoming data and provides an output MAC of the data.	Auth[2] (E) Encrypted Storage[2] (E) Customer Keys (E)
8	FCE Message Authentication (MAC)	X			This service provides an output MAC of the data.	CMAC FCE (E) HMAC FCE (E) Encrypted Storage[2] (E)
9	Signature Generation and Verification		X	X	This service creates signatures and verifies signatures.	Auth[2] (E) Encrypted Storage[2] (E) PUB_ES_ECC (E) PUB_ES_ECDH (E) PUB_ES_RSA (E) Customer Keys (E)
10	Encrypted storage[3] (key, data)		X	X	This service stores elements within the device in encrypted form as they are read or written through a GCM auth session.	Random KEK (E) CTR KEK (W)

#	Service	No Auth	User (Auth)	CO (Auth)	Description	Keys and CSPS/ Type(s) of Access R=read, W=write, E=execute, Z=zeroize
11	Certificate Extraction		X	X	This service extracts a public key from its certificate	Auth[2] (E) PUB_X509_Cert_ES (E) PUB_ES_Root (E) PUBK_X509 (W)
12	Storage (Data)	X[5]	X	X	This service stores elements within the device.	N/A
13	Secure Boot[4]		X	X	This service implements various phases of the secure boot process.	Auth[2] (E) PUB_ES_ECC (E) PUB_ES_ECDH (E) PUB_ES_RSA (E) PUBK_X509 (E)
14	Monotonic Counters	X	X	X	This service allows users to count activities within the device. This is not a cryptographic service and used for statistical purposes.	N/A
15	Random Number Generation	X	X	X	This service provides random numbers to the caller.	Entropy Input String (E) DRBG Input Seed (E) DRBG Internal State (E, Z)
16	TLS Session Establishment Support		X	X	This service provides support to external host for TLS session establishment (TLS 1.2)	Auth[2] (E) ECDH Shared secret Z (E, W, Z) SP800-56C Salt (E, W, Z) KDK (E, W, Z) Derived Key Material (W) TLS 1.2 KDF Internal State (E, W, Z) Encrypted Storage[2] (E) Customer Keys (E)
17	Storage Extension		X	X	This service allows data to be sent to external	Auth[2] (E) Encrypted Storage[2] (E)

#	Service	No Auth	User (Auth)	CO (Auth)	Description	Keys and CSPS/ Type(s) of Access R=read, W=write, E=execute, Z=zeroize
					storage and brought back into the device.	RPKK (E) Proof (W)
18	OAEP Encryption / Decryption		X	X	This service provides OAEP encryption/decryption.	Auth[2] (E) Encrypted Storage[3] (E) Customer Keys (E)
19	Cryptographic Self-Test	X	X	X	This service performs self-test of internal cryptographic algorithms	N/A
20	Secure Firmware Update[6]		X	X	This service allows firmware within the device to be updated.	MDUK (E) DevUpdate Key (E) DUPK (E)
21	CSP Zeroization		X	X	This service deletes all CSP material from the device.	RKEK (Z) RPKK (Z) MDUK (Z)
22	External Tamper Response[5]	X	X	X	This service deletes handles and resets the device initiated by external control input.	Customer Keys (Z)

Table 7-1 – Services and Access rights Authorized for Roles

Note[1]: The Module only supports two auth sessions at a given time.
Note[2]: Auth Identifies a list of common CSPs used during the Auth session service as a prerequisite for other services. See line “Auth Session”.
Note[3]: Encrypted Storage Identifies a list of common CSPs used during the encrypted storage service as a prerequisite for other services. See line “Encrypted Storage”.
Note[4]: The Secure Boot service shall **not** be used with full store mode.
Note[5]: This service is only available in TA100 59V01B6 based device part numbers.
Note[6]: The Secure Firmware Update service must only be applied to a CMVP validated version of firmware. Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Additional Note: the operator may create additional CO and User roles if desired. Both the COK and UAK users have the same set of services available.

8. Cryptographic Key Management

8.1. Secret Keys and CSPs

Description/Usage	Type	Generation	Establishment	Input/Output	Storage Persistent (NVM)/ Transient (SRAM)	Zeroization
Random KEK **(RKEK)**	HMAC SHA256 (128-bit key)	SP800-90A			Persistent: plaintext Transient: plaintext	Master Delete Command over-writes with DRBG output.
CTR KEK (8)	AES-128 CTR key (SP800-38A)	SP800-108 (from RKEK)			Persistent: N/A Transient: plaintext	Decrypted plaintext over-written during power-up
Random Proof KDF Key **(RPKK)**	HMAC SHA256 (128-bit key)	SP800-90A			Persistent: plaintext Transient: plaintext	Master Delete Command over-writes with DRBG output.
Proof Key	AES-128 GCM key (SP800-38D)	SP800-108 (from RPKK)			Persistent: N/A Transient: plaintext	Decrypted plaintext over-written during power-up
Crypto Officer Key **(COK T=0)**	GCM 128			Input: plaintext during manual distribution and electronic entry. Output: N/A	Persistent: via CTR KEK Transient: plaintext	Decrypted plaintext over-written during power-up
Provisional Session Key **(PSK)**	GCM 128	SP800-108 (from COK T=0)			Persistent: N/A Transient: encrypted by CTR_KEK	Explicitly zeroized at session termination
Other Crypto Officer Key(s) **(COK2)**	GCM 128	SP800-108 (from COK T=0)		Input: via GCM PSK Output: via GCM PSK	Persistent: via CTR KEK Transient: plaintext	Decrypted plaintext over-written during power-up
User Authorization Keys **(UAK)**	GCM 128	SP800-108 (from COK2)		Input: via GCM COK2 Output: via GCM COK2	Persistent: via CTR KEK Transient: plaintext	Decrypted plaintext over-written during power-up
Authorization Session Keys **(ASK)**	GCM 128	SP800-108 (from UAK or other COKs)			Persistent: N/A Transient: encrypted by CTR_KEK	Explicitly zeroized at session termination
Customer Keys	AES-128 ECB (ACE)	SP800-90A		Input: via GCM ASK or Proof Key	Persistent: via CTR KEK Transient: plaintext	Decrypted plaintext over-written during power-up

				Output: via GCM ASK or Proof Key		
	HMAC SHA256 (ACE) (16 through 64)	SP800-90A		Input: via GCM ASK or Proof Key Output: via GCM ASK or Proof Key	Persistent: via CTR KEK Transient: plaintext	Decrypted plaintext over-written during power-up
	CMAC (ACE) 128	SP800-90A		Input: via GCM ASK or Proof Key Output: via GCM ASK or Proof Key	Persistent: via CTR KEK Transient: plaintext	Decrypted plaintext over-written during power-up
	GCM 128	SP800-90A		Input: via GCM ASK or Proof Key Output: via GCM ASK or Proof Key	Persistent: via CTR KEK Transient: plaintext	Decrypted plaintext over-written during power-up
	ECC ECDSA 224,256,384 SHA256	SP800-90A, FIPS 186-4		Input: via GCM ASK or Proof Key Output: Proof Key	Persistent: via CTR KEK Transient: plaintext	Decrypted plaintext over-written during power-up
	ECDSA Per Message Secret "K"	SP800-90A, FIPS 186-4			Persistent: N/A Transient: plaintext	Decrypted plaintext over-written during power-up
	ECC ECDH 224,256,384	SP800-90A, SP800-56A		Input: via GCM ASK or Proof Key Output: N/A	Persistent: via CTR KEK Transient: plaintext	Decrypted plaintext over-written during power-up
	RSA PSS 2048 SHA256	SP800-90A, FIPS 186-4		Input: via GCM ASK or Proof Key Output: Proof Key	Persistent: via CTR KEK Transient: plaintext	Decrypted plaintext over-written during power-up
	RSA PKCS 1v5 2048 SHA256	SP800-90A, FIPS 186-4		Input: via GCM ASK or Proof Key Output: Proof Key	Persistent: N/A Transient: plaintext	Decrypted plaintext over-written during power-up
ECDH Shared Secrets (Z)	224,256,384		SP800-56Ar3		Persistent: N/A Transient: plaintext	Explicitly zeroized at session termination
SP800-56Cr1 Salt	HMAC SHA256			Input: via GCM ASK or Proof Key Output: N/A	Persistent: N/A Transient: plaintext	Explicitly zeroized at session termination
Key Derivation Key **(KDK)**	Key Derivation Key		SP800-56Cr1 HMAC SHA256		Persistent: N/A Transient: plaintext	Explicitly zeroized at session termination

Derived Key Material	Derived Key Material HMAC AES 128 128-1024		SP800-56Cr1 SP800-108	Input: N/A Output: via GCM ASK	Persistent: via CTR KEK Transient: plaintext	Decrypted plaintext over-written during power-up
SP800-56Cr1 KDF Internal State	HMAC-SHA256	SP800-56Cr1 KDF			Persistent: N/A Transient: plaintext	Explicitly zeroized at session termination
Master DevUpdate Key **(MDUK)**	HMAC SHA256 (128-bit key)				Persistent: plaintext Transient: plaintext	Master Delete Command over-writes with DRBG output
DevUpdate Key	AES-128 GCM key (SP800-38D)	SP800-108 (from MDUK)			Persistent: N/A Transient: plaintext	Decrypted plaintext over-written during power-up
Entropy Input String	Output of ENT (P)	SP800-90B ENT (P)			Persistent: N/A Transient: plaintext	Master Delete Command over-writes with DRBG output
DRBG Input Seed	AES-128 CTR	SP800-90B ENT (P)			Persistent: N/A Transient: plaintext	Master Delete Command over-writes with DRBG output
DRBG Internal State	Internal state values DRBG (V, Key) each pram is 128 bits.	SP800-90B ENT (P)			Persistent: N/A Transient: plaintext	Master Delete Command over-writes with DRBG output
SP800-108 KDF Internal State	HMAC SHA256		SP800-108 KDF		Persistent: N/A Transient: plaintext	Decrypted plaintext over-written during power-up
TLS 1.2 Pre-Master Secret	ECDH 224, 256, 384 bits	SP800-90A	SP800-56Ar3	Input: via GCM ASK Output: via GCM ASK	Persistent: N/A Transient: via CTR KEK	Decrypted plaintext over-written during power-up
TLS 1.2 Master Secret	ECDH 384 bits		SP800-135 KDF	Input: via GCM ASK Output: via GCM ASK	Persistent: N/A Transient: via CTR KEK	Decrypted plaintext over-written during power-up
TLS 1.2 Derived Keying Material	256-1024		SP800-135 KDF	Input: N/A Output: via GCM ASK	Persistent: N/A Transient: via CTR KEK	Decrypted plaintext over-written during power-up
TLS 1.2 KDF Internal State	HMAC SHA256		SP800-135 KDF		Persistent: N/A Transient: plaintext	Decrypted plaintext over-written during power-up
CMAC FCE	CMAC 128	SP800-90A		Input: via GCM ASK Output: via GCM ASK	Persistent: via CTR KEK Transient: plaintext	Decrypted plaintext over-written during power-up
HMAC FCE	HMAC SHA256	SP800-90A		Input: via GCM ASK Output: via GCM ASK	Persistent: via CTR KEK Transient: plaintext	Decrypted plaintext over-written during power-up

Table 8-1 – Description of the Cryptographic Private Keys and CSPs

8.2. Public Keys

Description/Usage	Type	Generation	Input/Output	Storage
ECC-P384, P256, P224 externally supplied **(PUB_EC_ECC)**	ECDSA		Input: via GCM ASK Output: via GCM ASK	plaintext
ECC-P384, P256, P224 Transient Output associated with private key gen **(PUB_TOPKG_ECC)**		ANS X9.62-2005 FIPS 186-4	Input: N/A Output: via GCM ASK	N/A
ECDH-P384, P256, P224 externally supplied **(PUB_ES_ECDH)**	ECDH		Input: via GCM ASK Output: via GCM ASK	plaintext
ECDH-P384, P256, P224 Transient Output associated with private key gen **(PUB_TOPKG_ECDH)**		SP800-56A	Input: N/A Output: via GCM ASK	N/A
RSA 2048, 3072 externally supplied **(PUB_ES_RSA)**	RSASSA-PKCS1-V1_5, RSASSA-PSS		Input: via GCM ASK Output: via GCM ASK	Plaintext
RSA 2048 Transient Output associated with private key gen **(PUB_TOPKG_RSA)**		RFC 3447 PKCS#1 v2.1 FIPS 186-4 including section 5.5 "PKCS #1"	Input: N/A Output: via GCM ASK	N/A
X.509 Certificate externally supplied **(PUB_X509_Cert_ES)**	RSA2048, ECC-P256		Input: Traceable to root public keys Output: Traceable to root public keys	Plaintext
Public key extracted from X.509 Certificate **(PUBK_X509)**	RSA2048, RSA3072, ECC-P256		Input: N/A Output: via GCM ASK	Plaintext
Root public keys externally supplied **(PUB_ES_Root)**			Input: plaintext Output: plaintext	Plaintext
DevUpdate Public Key **(DUPK)**	ECDSA P256		Input: N/A Output: plaintext	plaintext

Table 8-2 – Description of the Public Keys

9. Identification and Authentication Policy

9.1. Roles and Authentication

Role	Type of Authentication	Authentication Data	Description
Crypto Officer (CO)	Role Based	128 bit key	The services provided under the CO Role require the operator to authenticate to the TA100 device as the "owner". The CO services are used to initialize/configure the device and to install users and grant service permissions using the Auth Session (Auth) service.
User	Role Based	128 bit key	The services provided under the User Role require the operator to authenticate to the TA100 as an "entity". The User services obtain cryptographic or protected capability functions from the device based upon the permissions defined by the CO.
No Authentication Required (No Auth)	Implicit (none)	None	The authorized services provided under this role do not require any authentication. Authorization for assuming this role is implicit. The No Auth Required services do not require the use of protected capability functions (i.e. functions that require the use of CSPs associated with the CO or User). The list of No Authentication Required services is identified in the full list of services.

Table 9-1 - Roles and Required Identification and Authentication

The TA100 invokes a two-step process for services requiring role authentication. The first step is to open an authorization session. The second step is to authenticate the entity that is to be used.

Upon power-cycling the module will require the operator to reauthenticate to the module.

9.2. Strength of Authentication Mechanism

For Authentication using a 128 bit AES-GCM key which has a minimum equivalent computational resistance to attack of 2^128. Thus, the probability of a successful random attempt is 1/ (2^128), which is less than 1/1,000,000. The maximum number of back to back authentications which can be attempted in one minute, using the fastest communication interface of the device (16MHz SPI) is approximately 17,142 authentications per minute. Therefore, the probability of a successful random attempt per minute is 17,142/2^128 which is less than 1/100,000

Authentication Mechanism	Probability of Random Success	Probability of Random Success per Minute
AES-GCM	1/(2^128)	17,142/2^128

Table 9-2 - Strengths of Authentication Mechanisms

10. Physical Security Policy

The module meets the FIPS 140-2 Physical Security Level 3 requirements with Environmental Failure Protection.

The secret keys and CSPs are physically protected from unauthorized disclosure and/or modification. The module implements hardware and firmware security mechanisms to prevent environmental (voltage and temperature) failures and physical attacks. All secret keys and CSPs in the module's internal memory are encrypted.

The module is embedded within a production grade IC package which has a hard opaque tamper evident coating with standard passivation. The coating protects the module against environmental or other physical damage and attempts to remove the coating will leave evidence of tampering.

The module has internal sensors that detect variations in voltage and temperature that exceed the parametric limitations, either high or low. In the event that one of these sensors trigger an out-of-bounds condition, the module will shut down.

The normal operating range for the module is:

- Voltage: between 2.7V and 5.5V
- Temperature: between -40C and 125C

Hardness testing was only performed at ambient temperature. No assurance is provided for Level 3 hardness conformance at any other temperature.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Environmental Failure Protection	Performed automatically by the module.	The module will shutdown when it detects variations in voltage and temperature that exceed the parametric limitations.

Table 10-1 – Inspection/Testing of Physical Security Mechanisms

11. Operational Environment

The cryptographic module resides in a fixed operational environment. It is not possible to physically or logically alter the executable instructions and logic that reside within the cryptographic boundary.

12. Self-Tests

The module implements the following Self-tests.

12.1. Power-Up Self-Tests

ALGORITHM	Test Description
AES	Encrypt only ECB using 128-bit key KAT
AES-CMAC	Generate/verify using 128-bit key KATs
AES-GCM	Encrypt/decrypt using 128-bit key KATs
CRC-16	Integrity check
DRBG	AES-128 counter mode DRBG KAT (instantiate, generate and reseed) per SP800-90A Section 11.3
ENT (P) (SP800-90B)	Repetition Count Test and Adaptive Proportion Test over 1024 consecutive samples
ECDH	KAS KAT
ECDSA	Generate/Verify using 256-bit key KATs
HMAC	HMAC-SHA-256 KAT
RSA	PKCS#1 (v1.5) using 2048-bit key and SHA-256 KAT
SHA-256	KAT
SP800-108 KBKDF	HMAC-SHA-256 Counter Mode KAT
TLS V1.2 KDF PRF	HMAC-SHA-256 KAT

Table 12-1– Power-up Self-tests

12.2. Conditional Self-Tests

ALGORITHM	Test Description
AES-128-GCM	Firmware Load Test
DRBG, AES-GCM, HMAC-SHA	KAT on WAKE
ENT (P) (SP800-90B)	Continuous Health Testing through Repetition Count Test and Adaptive Proportion Test over 1024 consecutive samples
ECDSA	Pairwise consistency test
RSA	Pairwise consistency test

Table 12-2– Conditional Self-tests

12.3. Critical Function Test

The TA100 performs a CRC-16 integrity check over specific NVM regions on all start-up, reset and wake from sleep events. CSP related elements that are checked in this region include the below list:

1. Startup
   1a. Fuse Row
      a. Chip calibration, obfuscation, and trim data
   1b. Config. Memory Region
      a. User configuration data[1]
   1c. Tester memory Region[1]
      a. MDUK (master device update key)
      b. DUPK (device update public key)
      c. RKEK (random KEK), RPKK (random proof KDF key)
      d. CTR KEK[8] (AES CTR mode key encryption keys)
      e. Device “Unique” seed used when calculating a session_id at power up

Note1: The On Demand Integrity Tests for the Tester Memory and User Configuration Data are performed by power-cycling the module.

13. EMI/EMC

The Microchip Trust Anchor TA100 is designed as a custom ASIC designed to be embedded into a set of electronic products which themselves would undergo standard EMI/EMC certification.

Per 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, the module is not subject to EMI/EMC regulations because it is a subassembly designed for incorporation by equipment manufacturer into another device.

14. Mitigation of Other Attacks

The module's mitigation of other attack mechanisms has not been evaluated as a part of this FIPS validation. No claim to the assurance of these mechanisms.

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

Table 14-1 – Mitigation of Other Attacks

15. Glossary

TERM	DESCRIPTION
AES	Advanced Encryption Standard, as specified in [FIPS 197]
AES-GCM	AES with Galois/Counter Mode
ANSI	American National Standards Institute
CAVP	Cryptographic Algorithm Validation Program
CERT	Certificate
CKG	Cryptographic Key Generation
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CTR	Counter
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
EC DH	Elliptic Curve Diffie-Hellman (Algorithm)
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman (NIST SP 800-56A)
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
FSM	Finite State Model
GCM	Galois Counter Mode (GCM) and GMAC Algorithm
HMAC	Keyed-Hash Message Authentication Code, as specified in [FIPS 198]
IG	Implementation Guidance
KAS	Key Agreement Schemes and Key Confirmation (NIST SP 800-56A)
KDF	Key Derivation Function
MAC	Message Authentication Code
MD5	Message Digest 5
N/A	Not Applicable
NIST	National Institute of Standards and Technology
ENT (P)	Physical Non-deterministic Random Bit Generator
PUB	Publication
RNG	Random Number Generator
RSA	Rivest Shamir Adleman Cryptographic System (FIPS 186-4)
RSA	Reversible Digital Signature Algorithm (FIPS186-2 and FIPS186-3 RSA)
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SP	NIST Special Publication
SSH	Secure Shell
TLS	Transport Layer Security

Table 15-1 – Specification of Acronyms and their Descriptions

16. Appendix - Crypto Officer and User Guidance

Crypto Officer Guidance

The Crypto Officer is responsible for configuring the module in FIPS Compliance mode, as well as, maintaining and administrating the operations of the module.
The services provided under the CO Role require the operator to authenticate to the TA100 device as the “owner”. The CO services are used to initialize/configure the device and to install users.

- Administrative functions:
  - The Crypto Officer is responsible for initializing and configuring the module to run in FIPS Mode of operation. FIPS mode configuration guidance is detailed in section 5.2 of the Security Policy,
  - The Crypto Officer is also responsible for installing users.
- Physical ports, and logical interfaces: The Crypto Officer has access to all the modules physical ports and logical interfaces.
- Procedures on how to administer the cryptographic module in a secure manner are detailed in section 5 of the security policy.
- Assumptions regarding user behavior that are relevant to the secure operation of the cryptographic module are detailed in section 5.3 of the security policy.

User Guidance

The User Guidance describes the security functions of the cryptographic module along with instructions, guidelines, and warnings for the secure use of the module.

- The User Approved security functions are detailed in Table 6 of the security Policy.
- Physical ports, and logical interfaces: The User has access to all the modules physical ports and logical interfaces.

All user responsibilities necessary for the secure operation of a cryptographic module are detailed in section 5.3 of the security policy.