Microchip Technology Inc

Microchip Trust Anchor TA101

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.0
June 11TH, 2026

Table of Contents

List of Tables

1 General

1.1 Overview

This document defines the non-proprietary cryptographic module security policy for the Microchip Trust Anchor TA101 Cryptographic Module, which is a single chip cryptographic module declared as a Hardware module. This security policy describes how the module meets FIPS 140-3 overall Level 2 security with Level 3 Physical Security requirements, and how to operate the module in a FIPS 140-3 mode. Details of the security levels are described in section 1.2 below.

1.2 Security Levels

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	2
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	3
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	2
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Microchip Trust Anchor TA101 Security Device (may also be referred to as the module or TA101) 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 TA101 securely stores keys for AES, SHA2, HMAC, CMAC, RSA, ECDSA, EDDSA and ECDH among other algorithms, supporting both 128-bit and 256-bit security strength functions. 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 TA101 device also implements AES-GCM, AES-CMAC and SHA-HMAC encryption and AES-GCM decryption.

Module Type: Hardware

Module Embodiment: Single Chip

Cryptographic Boundary:

The cryptographic boundary is defined as the periphery of a single chip represented in the below exhibit comprised of a single semiconductor die plus a designated package as defined in the table “Tested Module Identification – Hardware” in section 2.2.

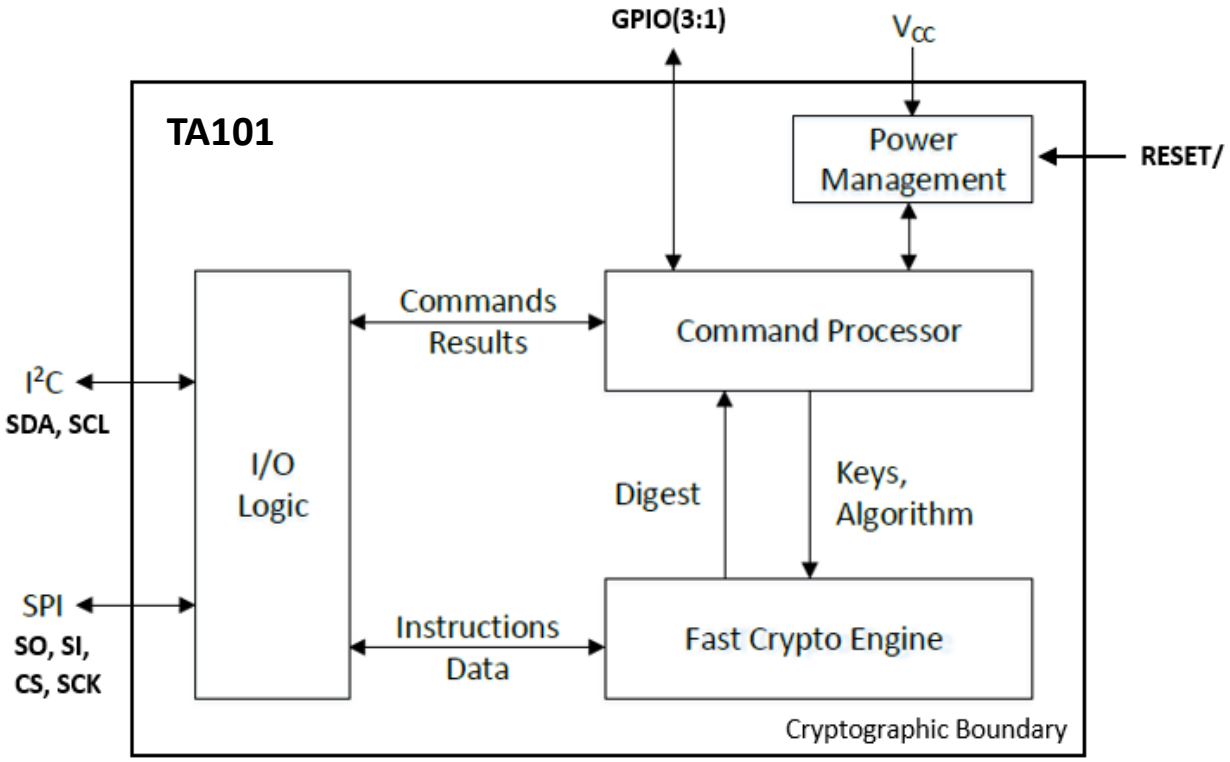

Exhibit 2-1 The Cryptographic Boundary and TOEPP of the Microchip Trust Anchor TA101

Tested Operational Environment’s Physical Perimeter (TOEPP):

The TOEPP is the physical perimeter of the Microchip Trust Anchor TA101 as defined by exhibit 2-1 above plus the designated page type defined in the table “Tested Module Identification – Hardware” in section 2.2.

The TA101 device is manufactured in three package configurations. The TA101 Hardware and Firmware versions implemented in the FIPS validated devices are identified in section “2.2 Tested and Vendor Affirmed Module Version and Identification”.

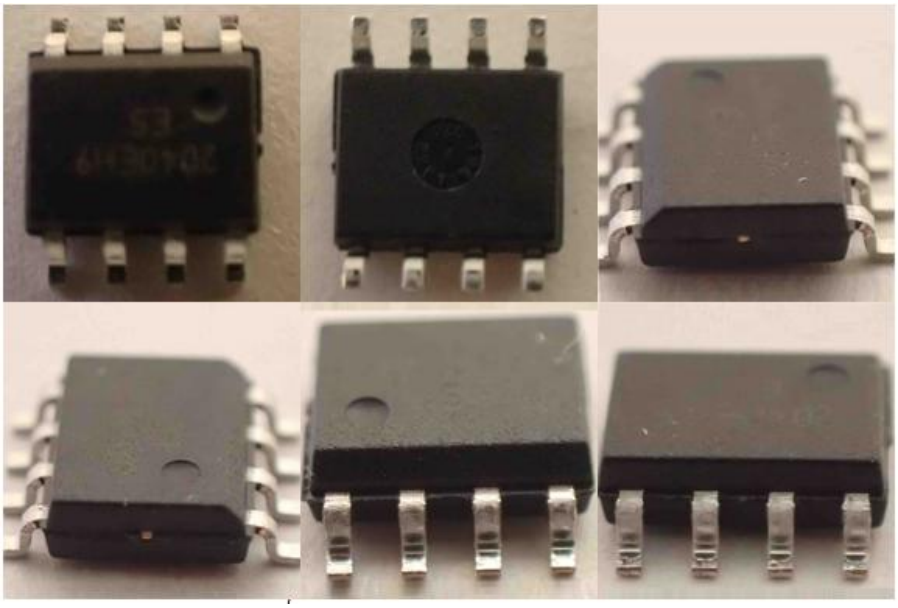

Exhibit 2-2 SOIC-8 TA101-Y250C2X01

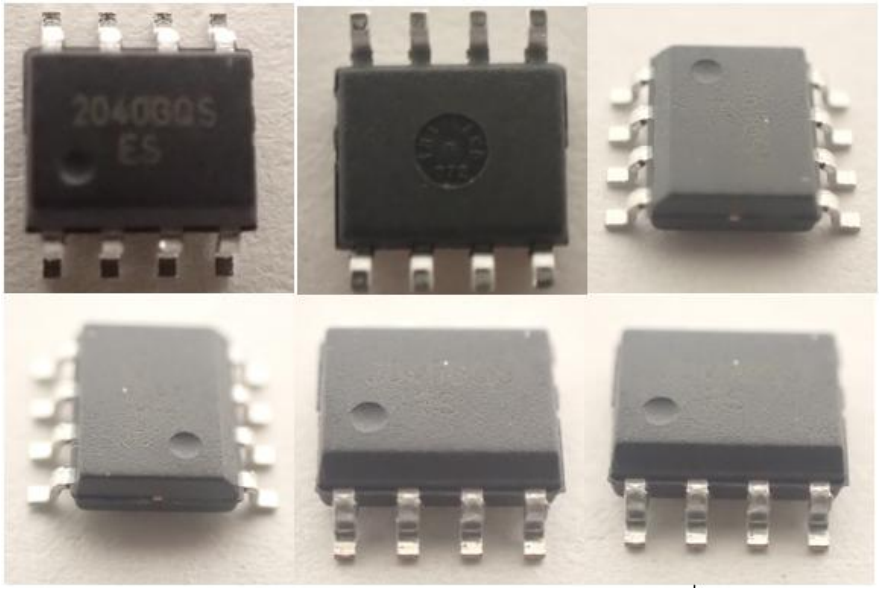

Exhibit 2-3 SOIC-8 TA101T-Y250C2X01

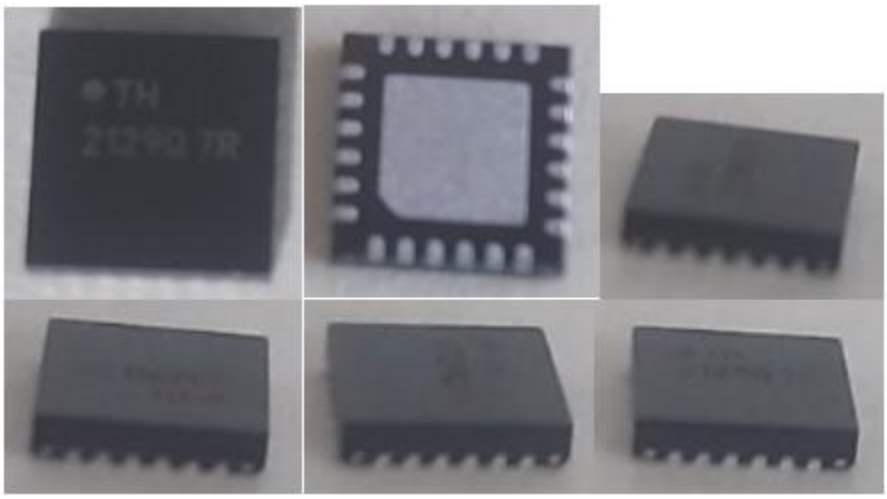

Exhibit 2-4 VQFN-24 TA101-Y250UFB01

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
TA101-Y250C2X01	59V01B9	CP ROM Ver 0x0001, ACE ROM Ver 0x01, DevUpdate Ver 0x00B90003	TA101 B9	SOIC-8 SPI
TA101T-Y250C2X01	59V01B9	CP ROM Ver 0x0001, ACE ROM Ver 0x01, DevUpdate Ver 0x00B90003	TA101 B9	SOIC-8 I2C
TA101-Y250UFB01	59V01B9	CP ROM Ver 0x0001, ACE ROM Ver 0x01, DevUpdate Ver 0x00B90003	TA101 B9	VQFN-24 SPI & I2C

Table 2: Tested Module Identification – Hardware

The Show Version – Status Service with Mode byte set to 0x00

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

Mode=0x00 Revision Information

Product Name	Description	ProdID	HWREV	0x00	CP ROM	Reserved	ACE ROM	Pkg_ID
Byte #		0	1	2	3	4:5	6	7
TA101	Current Version	0x01	0x02	0x00	0x01	0x0000	0x01	Varies see below

Exhibit 2-5 "Show version – Status" service – Output Response for Mode (0x00)

0x00 0x0D 0x00 **0x01 0x02 0x00 0x01** 0xXX 0xXX **0x01 0xPP** 0xXX 0xXX

Hardware revision 59V01B9:	Byte 0,1	0x0102
CP ROM revision:	Byte 2,3	0x0001
ACE ROM revision:	Byte 6	0x01
Package Type:	Byte 7	0xPP decoded to package type in the product datasheet

Note: Device package types supported by this security policy, Byte 7 (0xPP) may be 0x02 (TA101-Y250CX01: SOIC 8-pin with SPI interface), 0x03 (TA101T-Y250C2X01: SOIC 8-pin with I2C interface), or 0x04 (TA101-Y250UFB01: 24-VQFN with I2C and SPI Interface).

The Show Version – Status Service with Mode byte set to 0x07

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

0x00 0x15 0x00 0xXX 0xXX 0xXX 0xXX 0xXX 0xXX 0xXX 0xXX 0xXX 0xXX **0xB9 0x00 0x03 0x00** 0xXX 0xXX 0xXX 0xXX

DevUpdate NVM Code revision: Byte 10-13 0xB9000300 (as little endian 0x00B90003)

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 140-3 validation.

2.3 Excluded Components

The Module does not support excluded components.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Compliance	FIPS 140-3 Approved Mode of operation	Approved	Implicit indicator. The module only supports an Approved mode of operation.

Table 3: Modes List and Description

Degraded Mode Description:

The Module does not support a degraded mode.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CMAC	A6562	Direction - Generation, Verification Key Length - 128, 256	SP 800-38B
AES-CMAC	A874	Direction - Generation Key Length - 128	SP 800-38B
AES-CTR	A6463	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A6521	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A855	Direction - Encrypt Key Length - 128	SP 800-38A
AES-GCM	A6521	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.2 Key Length - 128, 256	SP 800-38D
AES-GMAC	A6521	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.2 Key Length - 128, 256	SP 800-38D
Counter DRBG	A6502	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A6542	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6542	Curve - P-224, P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6522	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6522	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
EDDSA KeyGen	A6528	Curve - ED-25519	FIPS 186-5
EDDSA KeyVer	A6528	Curve - ED-25519	FIPS 186-5
EDDSA SigGen	A6523	Curve - ED-25519 PreHash - Yes Pure - Yes	FIPS 186-5
EDDSA SigVer	A6523	Curve - ED-25519 PreHash - Yes Pure - Yes	FIPS 186-5
HMAC-SHA2-256	A6488	Key Length - Key Length: 256	FIPS 198-1
HMAC-SHA2-256	A853	Key Length - Key Length: 256	FIPS 198-1
HMAC-SHA2-384	A6488	Key Length - Key Length: 384	FIPS 198-1
HMAC-SHA2-512	A6488	Key Length - Key Length: 512	FIPS 198-1
KAS-ECC Sp800-56Ar3	A6594	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
		Function - Full Validation, Key Pair Generation Scheme - ephemeralUnified - KAS Role - Initiator, Responder KDF Methods - twoStepKdf - Key Length - 512	
KDF SP800-108	A6524	KDF Mode - Counter Supported Lengths - Supported Lengths: 128-1024 Increment 8	SP 800-108 Rev. 1
RSA KeyGen (FIPS186-5)	A6593	Key Generation Mode - probable Modulo - 2048, 3072, 4096 Primality Tests - 2pow100 Private Key Format - crt	FIPS 186-5
RSA SigGen (FIPS186-5)	A6527	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-5)	A6527	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
SHA2-256	A6451	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-256	A854	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-384	A6451	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-512	A6451	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A6525	Hash Algorithm - SHA2-256	SP 800-135 Rev. 1
TLS v1.3 KDF (CVL)	A6526	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE	SP 800-135 Rev. 1

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG			SP800-133r2 Sections - 4 Using the Output of a Random Bit Generator - 5 Generation of Key Pairs for Asymmetric – Key Algorithms - 5.1 Key Pairs for Digital Signature Schemes - 5.2 Key Pairs for Key Establishment - 5.3 Distributing the Key Pairs - 6 Generation of Keys for Symmetric – Key Algorithms - 6.1 The “Direct Generation” of Symmetric Keys - 6.2 Distributing the Generated Symmetric Key

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

Name	Caveat	Use and Function
LFSR (Non-FIPS)	FIPS 140-3 IG 2.4.A	Used for obfuscation within the crypto engine, dummy cycles, randomization for attack resistance
Masking / Blinding	FIPS 140-3 IG 2.4.A	Used for obfuscation of datapath information
Persistent Storage Obfuscator NVM	FIPS 140-3 IG 2.4.A	Used for obfuscation of data stored in NVM
Persistent Storage Obfuscator ROM	FIPS 140-3 IG 2.4.A	Used for obfuscation of data stored in ROM
Transport Pre-Key	FIPS 140-3 IG 2.4.A	Used for obfuscation of Master DevUpdate Key (MDUK), DevUpdate Public Key (DUPK) entry
Transport Key	FIPS 140-3 IG 2.4.A	Used to obfuscate manual entry during FIPS initialization
Transient Storage Obfuscator	FIPS 140-3 IG 2.4.A	Used for obfuscation of data stored in SRAM
Utility RNG	FIPS 140-3 IG 2.4.A	Used for NVM wear leveling or various obfuscation purposes

Table 6: Non-Approved, Allowed Algorithms with No Security Claimed

All of the above algorithms meet the caveat of FIPS 140-3 IG 2.4.A for acceptance of usage in the approved mode of operation in accordance with the defined criteria.

1) All of the above algorithms are not used in any manner to meet any FIPS 140-3 requirements.
2) All of the above algorithms do not access or share CSPs in a way that counters the requirements of this IG.
3) The following algorithms are not intended to be used as a security function and are used for NVM wear leveling or additional obfuscation of CSPs: “Utility RNG”.
4) The following algorithms are mathematical operations applied for “good measure” but not for providing sound security to obfuscate CSPs while performing device services: “LFSR (non-FIPS)”, “Masking / Blinding”, “Transport Pre-Key”, “Transport Key”.
5) The following algorithms are mathematical operations applied for “good measure” but not for providing sound security to obfuscate CSPs for persistent and non-persistent storage: “Persistent Storage Obfuscator NVM”, “Persistent Storage Obfuscator ROM”, “Transient Storage Obfuscator”.
6) All of the above algorithms are only used internally within the device with no operator interaction. Their non-approved use and purpose (from the above statements) is unambiguous to the operator and can’t be easily confused for a security function.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Auth Session Encryption	BC-Auth CKG	AES-GCM Tunnel created during an authorized session. Key establishment methodology provides 128 or 256 bits of encryption strength.		AES-GCM: (A6521) KDF SP800-108: (A6524) AES-GMAC: (A6521)
Internal encryption	BC-UnAuth	Internal encryption for storage.		AES-CTR: (A6463)
Key Exchange	KTS-Wrap	Write a key in an auth session.		AES-GCM: (A6521)
Key derivation	KAS-56CKDF KBKDF	Support for TLS1.2 PRF, TLS1.3 HKDF and 2 step KDF for Key Agreement Scheme.	Counter Length:8 bits	HMAC-SHA2-256: (A6488) HMAC-SHA2-384: (A6488) HMAC-SHA2-512: (A6488) TLS v1.2 KDF RFC7627: (A6525) TLS v1.3 KDF: (A6526)
Key generation	CKG AsymKeyPair-KeyGen	Generate Symmetric keys, ECC, and RSA Asymmetric Key pairs.		ECDSA KeyGen (FIPS186-5): (A6542) EDDSA KeyGen: (A6528) RSA KeyGen (FIPS186-5): (A6593)
HASH	SHA	Secure Hash Generation		SHA2-256: (A6451) SHA2-384: (A6451)

Name	Type	Description	Properties	Algorithms
				SHA2-512: (A6451)
CMAC	MAC	AES based Message Authentication Generation		AES-CMAC: (A6562)
HMAC	MAC	Secure Hash-Based Message Authentication Generation		HMAC-SHA2-256: (A6488) HMAC-SHA2-384: (A6488) HMAC-SHA2-512: (A6488)
FCE-MAC	MAC	Cryptographic support using hardware Fast Crypto Engine.		SHA2-256: (A854) HMAC-SHA2-256: (A853) AES-CMAC: (A874) AES-ECB: (A855)
Sign	DigSig-SigGen	Digital Signature Generation	KeyGen:Yes PureEd:Yes PreHashEd:Yes Ed_Context_Length:256	KAS-ECC Sp800-56Ar3: (A6594) EDDSA SigGen: (A6523) RSA SigGen (FIPS186-5): (A6527) ECDSA SigGen (FIPS186-5): (A6522)
Verify	DigSig-SigVer	Digital Signature Verification	KeyGen:Yes PureEd:Yes PreHashEd:Yes Ed_Context_Length :256	KAS-ECC Sp800-56Ar3: (A6594) EDDSA SigVer: (A6523) RSA SigVer (FIPS186-5): (A6527) ECDSA SigVer (FIPS186-5): (A6522) ECDSA KeyVer

Name	Type	Description	Properties	Algorithms
				(FIPS186-5): (A6542) EDDSA KeyVer: (A6528)
Export-encryption	KTS-Wrap	Export a Key blob		AES-GCM: (A6521) Key Length: 256 KDF SP800-108: (A6524)
Import-decryption	KTS-Wrap	Import a Key blob		AES-GCM: (A6521) Key Length: 256 KDF SP800-108: (A6524)
GCM-ENC	BC-Auth	Decrypts the Device update patch.	Key size:128 bits GCM Tag Length:128 bits Decrypt Operation:Yes	AES-GCM: (A6521) Key Length: 128 KDF SP800-108: (A6524)
Random	DRBG	Generate Random number using Internal DRBG.	DRBG:CTR_DRBG Prediction Resistance:Not Enabled Reseed:Not implemented Block Cipher: AES256 with DF	Counter DRBG: (A6502)
AES-Encrypt	BC-Auth BC-UnAuth	Encrypt user data using AES-GCM/ECB		AES-GCM: (A6521) Key Length: 128, 256 AES-ECB: (A6521) Key Length: 128, 256
AES-Decrypt	BC-Auth BC-UnAuth	Decrypt user data using AES-GCM/ECB		AES-GCM: (A6521) Key Length: 128, 256 AES-ECB: (A6521) Key Length: 128, 256

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

- **AES-GCM**
  - Per FIPS 140-3 IG C.H, the AES-GCM IV is generated inside the module's boundary via the Approved DRBG. The module generates a 96-bit IV. Upon loss of power a new IV is generated by the module.

2.8 RBG and Entropy

Cert Number	Vendor Name
E194	Microchip Technology Inc

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
TA NRBG Entropy Source	Physical	TA101 B9	1-bit	0.51	None

Table 9: Entropy Sources

The Counter DRBG produces random number outputs with 256-bit security strength.

The cryptographic module abides by the requirements of the public use document;

https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/entropy/E194_PublicUse.pdf

2.9 Key Generation

The module can generate Key material for both symmetric and asymmetric cryptographic algorithms. These keys are derived from an ESV certified NRBG and SP800-90A compliant DRBG-CTR and have up to 256 bits of security strength.
Refer to the entry - *Key generation* - in section 2.6 Security Function Implementations.

Additional notes:

- Key Generation shall only be performed inside an Authorization Session.
- Per FIPS 140-3 IG D.H, the module generates symmetric and asymmetric keys via the direct output of the DRBG.
- RSA and ECC keys shall only be generated using SP800-90A DRBG per FIPS 140-3 IG D.H (using SP800-56A is disallowed).
- For more information on SP 800-133r2 see table 5 Vendor-Affirmed Algorithms.

2.10 Key Establishment

This module supports Key establishment. The key establishment can be used as either stand-alone functionality or within a higher-level protocol such as TLS1.2 or TLS1.3.
Refer to the entry - *Key derivation* - in section 2.6 Security Function Implementations.

2.11 Industry Protocols

The Module conforms to 140-3 [IG] D.C References to the Support of Industry Protocols: while the module provides SP800-56Ar3 conformant schemes and API entry points oriented to TLS usage, the Module does not contain the full implementation of TLS. The following statements are required per IG D.C case #2:

> *No parts of the TLS protocol other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.*

2.12 Additional Information

The Module design corresponds to the Module security rules. Security rules enforced by the Module are described in the appropriate context of this document.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
GPIO_1	Status Output	External output interrupt source. Non-security status indicator.
GPIO_2	Status Output	External output interrupt source. Non-security status indicator.
GPIO_3	Control Input Status Output	External input: device wake or tamper source. External output: system reset or interrupt source. Non-security status indicator.
SDA	Data Input Data Output Control Input Status Output	I2C Data (input and output).
SCL	Control Input	I2C Clock.
CS/	Control Input	SPI Chip select, active low.
SI	Data Input Control Input	SPI Serial data input.
SCK	Control Input	SPI clock.
SO	Data Output Status Output	SPI Serial data output.
RESET/	Control Input	Reset Input, active low.
RESET2/	Control Input	Alternate Reset Input, active low.

Physical Port	Logical Interface(s)	Data That Passes
Vss	Power	Ground.
Vcc	Power	2.7 – 5.5V Power Supply.

Table 10: Ports and Interfaces

The module does not support Control Output.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Authentication	Authentication using a 128 bit or 256 bit AES-GCM key	AES-GCM	1/2^128	17142/2^128

Table 11: Authentication Methods

For Authentication using a 128-bit or 256-bit AES-GCM key which has a minimum equivalent computational resistance to attack of 2^128 or 2^256, respectively. Thus, the worst-case 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.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO	Role	Crypto Officer - The services provided under the CO Role require the operator to authenticate to the TA101 device as the “owner”.	Authentication
USER (CO2)	Role	Crypto Officer 2 -The services provided under the USER (CO2) Role require the operator to	Authentication

Name	Type	Operator Type	Authentication Methods
		authenticate to the TA101 as an “entity”.	
NO AUTH	Role	No Authentication Required - The authorized services permissible by this role do not require any authentication.	None

Table 12: Roles

The TA101 module requires 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.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Version - Status	This service provides device information and state.	CSR = xxx1 00x0	Status Request	Status Result	None	CO USER (CO2) NO AUTH
Power Management	This service manages the operating mode of the device relative to power.	CSR = 0000 0010. At next power up.	Request	None	None	CO - RKEK: Z - CTR KEK : Z - RPKK: Z - Proof Key: Z - COK: Z - COK2: Z - UAK: Z - ASK: Z - CKAES: Z - CKHMAC: Z - CKCMAC: Z - CKGCM: Z - CKECDSA: Z - CKECDSAK: Z - CKECDH: Z - CKRSA: Z - ECDH Shared Secrets (Z): Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SP800-56Cr2 Salt: Z - KDK: Z - Derived Key Material: Z - MDUK: Z - DevUpdate Key: Z - Entropy Input String: Z - DRBG Input Seed: Z - DRBG Internal State: Z - TLS 1.3 Salt: Z - TLS 1.3 Shared Secret Z: Z - TLS 1.3 KDK : Z - TLS 1.3 DerivedKeyingMaterial: Z - TLS 1.2 Pre-Master Secret: Z - TLS 1.2 Master Secret: Z - TLS 1.2 DerivedKeyingMaterial: Z - CMAC FCE: Z - HMAC FCE: Z - PUB_ES_ECC: Z - PUB_TOPKG_ECC: Z - PUB_ES_ECDH: Z - PUB_TOPKG_ECDH: Z - PUB_ES_RSA: Z - PUB_TOPKG_RSA: Z - PUB_ES_Root: Z - PUB_X509_Cert_

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ES: Z - PUBK_X509: Z - DUPK: Z USER (CO2) - RKEK: Z - CTR KEK : Z - RPKK: Z - Proof Key: Z - COK: Z - COK2: Z - UAK: Z - ASK: Z - CKAES: Z - CKHMAC: Z - CKCMAC: Z - CKGCM: Z - CKECDSA: Z - CKECDSAK: Z - CKECDH: Z - CKRSA: Z - ECDH Shared Secrets (Z): Z - SP800-56Cr2 Salt: Z - KDK: Z - Derived Key Material: Z - MDUK: Z - DevUpdate Key: Z - Entropy Input String: Z - DRBG Input Seed: Z - DRBG Internal State: Z - TLS 1.3 Salt: Z - TLS 1.3 Shared Secret Z: Z - TLS 1.3 KDK : Z - TLS 1.3 DerivedKeyingMaterial: Z - TLS 1.2 Pre-Master Secret: Z - TLS 1.2 Master

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Secret: Z - TLS 1.2 DerivedKeyingMaterial: Z - CMAC FCE: Z - HMAC FCE: Z - PUB_ES_ECC: Z - PUB_TOPKG_ECC: Z - PUB_ES_ECDH: Z - PUB_TOPKG_ECDH: Z - PUB_ES_RSA: Z - PUB_TOPKG_RSA: Z - PUB_ES_Root: Z - PUB_X509_Cert_ES: Z - PUBK_X509: Z - DUPK: Z NO AUTH - RKEK: Z - CTR KEK : Z - RPKK: Z - Proof Key: Z - COK: Z - COK2: Z - UAK: Z - ASK: Z - CKAES: Z - CKHMAC: Z - CKCMAC: Z - CKGCM: Z - CKECDSA: Z - CKECDSAK: Z - CKECDH: Z - CKRSA: Z - ECDH Shared Secrets (Z): Z - SP800-56Cr2 Salt: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- KDK: Z - Derived Key Material: Z - MDUK: Z - DevUpdate Key: Z - Entropy Input String: Z - DRBG Input Seed: Z - DRBG Internal State: Z - TLS 1.3 Salt: Z - TLS 1.3 Shared Secret Z: Z - TLS 1.3 KDK : Z - TLS 1.3 DerivedKeyingMaterial: Z - TLS 1.2 Pre-Master Secret: Z - TLS 1.2 Master Secret: Z - TLS 1.2 DerivedKeyingMaterial: Z - CMAC FCE: Z - HMAC FCE: Z - PUB_ES_ECC: Z - PUB_TOPKG_ECC: Z - PUB_ES_ECDH: Z - PUB_TOPKG_ECDH: Z - PUB_ES_RSA: Z - PUB_TOPKG_RSA: Z - PUB_ES_Root: Z - PUB_X509_Cert_ES: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- PUBK_X509: Z - DUPK: Z
Auth Session	This Service sets up an auth session to limit user service access	CSR = xxx1 00x0	Auth request, service	Encrypted service output , auth data	Auth Session Encryption	CO - COK: E - COK2: E - ASK: G,E,Z - RKEK: E - CTR KEK : G,E,Z USER (CO2) - UAK: E - ASK: G,E - RKEK: E - CTR KEK : G,E,Z
Data Element Creation	This service creates non-CSP elements in the shared data memory or a volatile register with specific attributes.	CSR= xxx1 00x0	Request	Success Code	None	CO USER (CO2)
SSP Element Creation	Creates SSP elements (private and public , symmetric and asymmetric) in the shared data memory or a volatile register with specific attributes.	CSR= xxx1 00x0	Request	Success Code	Internal encryption Key Exchange Key derivation Key generation Random	CO - PUB_TOPKG_ECC: G - PUB_TOPKG_RSA: G - COK2: W - UAK: W - RKEK: E - CTR KEK : G,E,Z - CKECDH: E - ECDH Shared Secrets (Z): G,W,Z - SP800-56Cr2 Salt: W,E,Z - KDK: G,E,Z - Derived Key Material: W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Entropy Input String: E - DRBG Input Seed: - DRBG Internal State: - CKECDSA: W - CKRSA: W - PUB_ES_RSA: W - PUB_ES_ECC: W - PUB_ES_Root: W - PUB_ES_ECDH: - PUBK_X509: W - PUB_X509_Cert_ES: W - PUB_TOPKG_ECDH: G USER (CO2) - CKECDH: E - ECDH Shared Secrets (Z): G,W,Z - SP800-56Cr2 Salt: W,E,Z - KDK: G,E,Z - Derived Key Material: W - Entropy Input String: E - DRBG Input Seed: E - DRBG Internal State: E - RKEK: E - CTR KEK : G,E,Z - CKECDSA: W - CKRSA: W - PUB_ES_RSA: W - PUB_ES_ECC: W - PUBK_X509: W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- PUB_X509_Cert_ES: W - PUB_ES_Root: W - PUB_ES_ECDH: W - PUB_TOPKG_ECC: G - PUB_TOPKG_ECDH: G - PUB_TOPKG_RSA: G
Message Authentication (MAC)	This service authenticates incoming data and provides an output MAC of the data.	CSR= xxx1 00x0	Data	MAC	CMAC HMAC	CO - RKEK: E - CTR KEK : G,E,Z - CKHMAC: E - CKCMAC: E USER (CO2) - RKEK: E - CTR KEK : G,E,Z - CKHMAC: E - CKCMAC: E
FCE Message Authentication (MAC)	This service provides an output MAC of the data.	FSR=00 x1 xxx0	Data	MAC	FCE-MAC	NO AUTH - CMAC FCE: E - HMAC FCE: E - RKEK: E - CTR KEK : G,E
Message Hash	This service hashes the data.	CSR= xxx1 00x0	Data	Hash	HASH	CO USER (CO2) NO AUTH
Signature Generation	This service creates digital signatures	CSR= xxx1 00x0	Message	Signature	HASH Sign Random	CO - CKECDSA: E - CKECDSAK: E - CKRSA: E - RKEK: E - CTR KEK : G,E USER (CO2) - CKECDSA: E - CKECDSAK: E - CKRSA: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- RKEK: E - CTR KEK : G,E
Signature Verification	This service creates verifies digital signatures.	CSR=xxx100x0	signature, message	Success/Fail	HASH Verify	CO - PUB_ES_ECC: E - PUB_ES_RSA: E - PUB_ES_Root: E - PUB_X509_Cert_ES: E - PUBK_X509: E USER (CO2) - PUB_ES_ECC: E - PUB_ES_RSA: E - PUB_ES_Root: - PUB_X509_Cert_ES: - PUBK_X509: E
Certificate Extraction	This service extracts a public key from its certificate.	CSR=xxx100x0	Certificate	Public key	Verify	CO - PUB_ES_Root: E - PUB_X509_Cert_ES: E - PUBK_X509: G,W USER (CO2) - PUB_ES_Root: E - PUB_X509_Cert_ES: E - PUBK_X509: G,W
Storage (Data)	Stores elements within the device.	CSR=xxx100x0	Data	Success Code	None	CO USER (CO2) NO AUTH
Secure Boot Setup	This service imports secure boot validation data.	CSR=xxx100x0	Validation data	Success Code	Verify	CO - COK: E - COK2: E - ASK: G,E - PUB_ES_ECC: E - PUB_ES_RSA: E - PUB_X509_Cert_ES: E USER (CO2)

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- UAK: E - ASK: G,E - PUB_ES_ECC: E - PUB_ES_RSA: E - PUB_X509_Cert_ES: E
Secure Boot update	This service updates secure boot validation data	CSR=xxx100x0	Validation data	Success Code	Verify	CO - PUB_ES_ECC: E - PUB_ES_RSA: E - COK: E - COK2: E - ASK: G,E - PUB_X509_Cert_ES: E USER (CO2) - PUB_ES_ECC: E - PUB_ES_RSA: E - ASK: G,E - UAK: E - PUB_X509_Cert_ES: E
Secure Boot execute	This service validates secure boot validation data	CSR=xxx100x0	Data to be validated	Success Code	Verify	CO - PUB_ES_ECC: E - PUB_ES_RSA: - COK: E - COK2: E - ASK: G,E - PUB_X509_Cert_ES: E USER (CO2) - PUB_ES_ECC: E - PUB_ES_RSA: E - PUB_X509_Cert_ES: E - UAK: E - ASK: G,E
Monotonic Counters	Allows users to count activities	CSR=xxx100x0	Request increment, Request	Success Code, Count Value	None	CO USER (CO2) NO AUTH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	within the device.		Read Value			
Random Number Generation	This service provides random numbers to the caller.	CSR=xxx100x0	Request	Random number	Random	CO - Entropy Input String: E - DRBG Input Seed: E - DRBG Internal State: E USER (CO2) - Entropy Input String: E - DRBG Input Seed: E - DRBG Internal State: E NO AUTH - Entropy Input String: E - DRBG Input Seed: E - DRBG Internal State: E
TLS Session Establishment Support	This service provides support to external host for TLS session establishment (TLS 1.2 or TLS 1.3)	CSR=xxx100x0	Handshake	Session Key	Key Exchange Key derivation Key generation HASH Sign Verify Random AES-Encrypt AES-Decrypt	CO - COK: E - COK2: E - ASK: G,E - TLS 1.3 Salt: E - TLS 1.3 Shared Secret Z: G,E - TLS 1.3 KDK : G,E - TLS 1.3 DerivedKeyingMaterial: G,E - TLS 1.2 Pre-Master Secret: G,E - TLS 1.2 Master Secret: G,E - TLS 1.2 DerivedKeyingMaterial: G,E USER (CO2) - UAK: E - ASK: G,E - TLS 1.3 Salt: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS 1.3 Shared Secret Z: G,E - TLS 1.3 KDK : G,E - TLS 1.3 DerivedKeyingMaterial: G,E - TLS 1.2 Pre-Master Secret: G,E - TLS 1.2 Master Secret: G,E - TLS 1.2 DerivedKeyingMaterial: G,E
Storage Extension	Allows data to be sent to external storage and brought back into the device.	CSR= xxx1 00x0	Request and identifier or Enc Blob	Enc Blob or success code	Export-encryption Import-decryption Random	CO - RPKK: E - Proof Key: G,E - CMAC FCE: R - HMAC FCE: R - RKEK: E - CTR KEK : G,E - CKECDSA: R - CKRSA: R - PUB_ES_ECC: R - PUB_ES_ECDH: R - PUB_ES_RSA: R - PUB_ES_Root: R - PUB_X509_Cert_ES: R - PUBK_X509: R USER (CO2) - RPKK: E - Proof Key: G,E - CMAC FCE: R - HMAC FCE: R - RKEK: E - CTR KEK : G,E - CKECDSA: R - CKRSA: R - PUB_ES_ECC: R - PUB_ES_ECDH: R - PUB_ES_RSA: R - PUB_ES_Root: R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- PUB_X509_Cert_ES: R - PUBK_X509: R
Cryptographic Self-Test	Performs self-test of internal cryptographic algorithms	CSR= xxx1 00x0	Request	Success code	Key Exchange Key derivation Key generation HASH CMAC HMAC FCE-MAC Sign Verify GCM-ENC Random AES-Encrypt AES-Decrypt	CO USER (CO2) NO AUTH
Secure Firmware Update	Allows firmware within the device to be updated.	CSR = 0000 0010	New Code	Reset, new version reported	Verify GCM-ENC HASH	CO - MDUK: E - DevUpdate Key: G,E - RKEK: E - CTR KEK : G,E
Zeroize	This service zeroizes all SSP material from the device	CSR= xxx1 00x0	Request	Success code	None	CO - RKEK: Z - RPKK: Z - COK: Z - MDUK: Z - Entropy Input String: E - DRBG Input Seed: E - DRBG Internal State: E

Table 13: Approved Services

Note: The operator may create additional CO and USER (CO2) roles if desired. Both the COK and UAK users have the same set of services available.
Note: The Module only supports two auth sessions at a given time.
Note: The Secure Boot service shall **not** be used with full store mode.
Note: Per FIPS 140-3 IG 2.4.C Approved Security Service Indicator, a claim is made that this module uses technique #2 for "Global Indicator".

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

The Secure Firmware Update service must only be applied to a CMVP validated version of firmware.

4.6 Bypass Actions and Status

The Module does not support Bypass Actions.

4.7 Cryptographic Output Actions and Status

The module supports self-initiated cryptographic output capability for the FCE Message Authentication (MAC) service.

The following independent actions by a Crypto Officer are required for the FCE to be in this mode.

1. Independent Action #1: A Crypto Officer must establish an Auth session. After which, valid keys must be imported by a Crypto Officer into the device's internal memory.
2. A Crypto Officer requests the FCE module enablement.
3. Independent Action #2: The module validates the FCE request. If valid, the module enables the FCE.
4. A Crypto Officer reads the status of the initializing commands to verify that the preparation steps have been executed successfully. The self-initiated cryptographic output capability is ready for use.
5. Any operator may read the Fast Crypto Status register (FSR) "F_INIT" bit to verify that the FCE has been initialized and the FCE has been configured for self-initiated cryptographic output capability.

This FCE MAC service and its configuration is not preserved over resetting, rebooting, or power cycling of the module.

5 Software/Firmware Security

5.1 Integrity Techniques

Integrity testing is performed over two separate regions of the internal NVM memory, by two separate tests. Each test is an EDC CRC-16 integrity check.

1) NVM Patch Code Integrity Test (CRC-16)
   a. Performs an integrity test over the executable patch code region of the NVM memory on power-up.
2) NVM Configuration Integrity Test (CRC-16)

a. Performs an integrity test over critical SSP elements in the NVM configuration region on all power-up, reset and wake from sleep events.
b. SSP related elements that are checked in this region include the below list:
    i. Chip calibration, obfuscation, and trim data
    ii. User configuration data
    iii. Tester memory Region data
        1. MDUK (master device update key)
        2. DUPK (device update public key)
        3. RKEK (random KEK), RPKK (random proof KDF key)
        4. CTR KEK[8] (AES CTR mode key encryption keys)
        5. Device “Unique” seed used when calculating a session id at power up

5.2 Initiate on Demand

1. NVM Patch Code Integrity Test – initiated by power-cycling the module.
2. NVM Configuration Integrity Test – initiated by power-cycling the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied:

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.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Environmental Failure Protection	Performed automatically and continuously by the module.	The module will shut down when it detects variations in voltage and temperature that exceed the parametric limits.

Table 14: Mechanisms and Actions Required

The parametric limits of the module’s normal operating range are 2.7V < Vcc < 5.5V and -40C <Ta < +125C.

The module meets the FIPS 140-3 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.

7.5 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
HighVoltage	5.5V	EFP	Device Reset
LowVoltage	2.7V	EFP	Device Reset
HighTemperature	125C	EFP	Device Reset
LowTemperature	-40C	EFP	Device Reset

Table 15: EFP/EFT Information

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

7.6 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-65C
HighTemperature	150C

Table 16: Hardness Testing Temperatures

8 Non-Invasive Security

8.1 Mitigation Techniques

Please see Section 12 for the module's mitigation of other attack mechanisms.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
SRAM	SRAM of the ACE	Dynamic
NVM EEPROM	Non-Volatile Memory	Static

Table 17: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Auth Session In Bound	Outside	NVM	Encrypted	Automated	Electronic	Auth Session Encryption
Auth Session Outbound	NVM	Outside	Encrypted	Automated	Electronic	Auth Session Encryption
Manufacturing-Input	Outside	NVM	Plaintext	Manual	Direct	

Table 18: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
SRAM Zeroization	After completion of the service, the SSP used is cleared from volatile memory.	The space containing the SSP is replaced with 0's, making retrieval impossible.	Enforced automatically by the module
Master Delete	Zeroizes the NVM space	The NVM space containing SSP's is replaced with 0's, making retrieval impossible.	Initiated through the Zeroize service

Table 19: SSP Zeroization Methods

Note: After the Master Delete (Zeroize service) is run, operators can use one of the following methods to identify that the zeroization method has successfully been completed.

1) Observance of the devices' usual "command has completed" response coming out of the device.

2) Run the "Show Version - Status" service to observe that the Zeroize service command has finished.

Note that if the Zeroize service did not complete, the operator will not be able to run the "Show Version - Status" service until the Zeroize service completes. They should wait for the Zeroize service to be completed.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
RKEK	KDK SP800-108 KDF (Unique value per part)	128 - 128	HMAC SHA 256 - CSP	N/A (SP800-90A at manufacturing)		Internal encryption
CTR KEK	Unique key per handle	128 - 128	AES-128 CTR key (SP800-38A) - CSP	KDF SP800-		Internal encry

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
				108 (A6524)		ption Key generation Sign
RPKK	Used to bind a blob to each unique TA101 module.	128 - 128	128-bit key used in KDKDF - CSP	N/A (SP800-90A at manufacturing)		Internal encryption
Proof Key	Key Encryption Key using AES-256 GCM	256 - 128*	AES-256 GCM Key - CSP	KDF SP800-108 (A6524)		Export-encryption Import-decryption
COK	Crypto Officer Key loaded in during manufacturing	128/256 - 128/256	Authentication - CSP	N/A - Installed during manufacturing		Auth Session Encryption
COK2	Secondary Crypto Officer key loaded using COK Auth session	128/256 - 128/256	Authentication - CSP	Counter DRBG (A6502)		Auth Session Encryption
UAK	User Auth Key loaded using COK/COK2 Auth session	128/256 - 128/256	Authentication - CSP	Counter DRBG (A6502)		Auth Session Encryption
ASK	generated Auth session key	128/256 - 128/256	AES-128/256 GCM key - CSP	KDF SP800-108 (A6524)		Key Exchange Key derivation Key gener

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						ation HASH CMAC HMAC Sign Verify Export-encryption Import-decryption GCM-ENC AES-Encrypt AES-Decrypt
CKAES	Customer Keys - AES	128/256 - 128/256	AES 128/256 ECB - CSP	Counter DRBG (A6502)		AES-Encrypt AES-Decrypt
CKHMAC	Customer Keys - HMAC	256 to 1024 - 256	HMAC-SHA256/384/512 - CSP	Counter DRBG (A6502)		HMAC
CKCMAC	Customer Keys - CMAC	128/256 - 128/256	AES CMAC 128/256 - CSP	Counter DRBG (A6502)		CMAC
CKGCM	Customer Keys - GCM	128/256 - 128/256	AES GCM 128/256 - CSP	Counter DRBG (A6502)		AES-Encrypt
CKECDSA	Customer Keys - ECC	224/256/384/521/256/256 - 112/128/192/256/128/128	ECC ECDSA (P-224,P-256,P-384,P-521,brainpoolP256r1), EDDSA (Ed25519) - CSP	Counter DRBG (A6502) ECDSA KeyGen (FIPS18		Key generation Sign

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
				6-5) (A6542)		
CKECDSAK	ECDSA per message secret "K"	224/256/384/521/256 - 112/128/192/256/128	ECC ECDSA (P-224,P-256,P-384,P-521,brainpoolP256r1) - CSP	Counter DRBG (A6502) ECDSA KeyGen (FIPS186-5) (A6542)		Sign
CKECDH	Customer Keys - ECDH	224/256/384/521/256 - 112/128/192/256/128	ECDH (P-224,P-256,P-384,P-521,brainpoolP256r1) - CSP	Counter DRBG (A6502) KAS-ECC Sp800-56Ar3 (A6594)		Key Exchange
CKRSA	Customer Keys - RSA	2048/3072/4096 - 112/128/140	RSA(2048,3072,4096) - CSP	Counter DRBG (A6502) RSA KeyGen (FIPS186-5) (A6593)		Key generation Sign
ECDH Shared Secrets (Z)	Output of ECDH command	224/256/384/521 - 112/128/192/256	SP800-56Ar3 - CSP		KAS-ECC Sp800-56Ar3 (A6594)	Key Exchange Key derivation
SP800-56Cr2 Salt	HMAC Key for randomness extraction in 2 step KDF	256 - 256	SP800-56cr2 two step KDF HMAC - CSP			Key Exchange Key derivation
KDK	Key Derivation Key - Randomness Extraction output in two step KDF used in	256/384/512 - >=256	HMAC - CSP		KAS-ECC Sp800-56Ar3 (A6594)	Key Exchange Key derivation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	ECDH-Public key establishment scheme					
Derived Key Material	Key Expansion output in two step KDF used in ECDH-Public key establishment scheme	256 to 1024, 128/256 - >=256, 128/256	HMAC,AES - CSP		KAS-ECC Sp800-56Ar3 (A6594)	Key Exchange Key derivation
MDUK	Master DevUpdate Key	128 - 128	HMAC - CSP	N/A. Installed during manufacturing		GCM-ENC
DevUpdate Key	Key derived from Master DevUpdate key	128 - 128	AES-GCM - CSP	KDF SP800-108 (A6524)		GCM-ENC
Entropy Input String	The raw output of the NRBG that is input to CTR-DRBG derivation function.	512 - 256	NRBG - CSP	Random		Key generation Random
DRBG Input Seed	Output of CTR-DRBG derivation function(entropy_input (512), nonce (256))	768 - 256	CTR-DRBG - CSP	Counter DRBG (A6502)		Random
DRBG Internal State	The internal state of the DRBG (V (128), Key (256)).	384 - 256	CTR-DRBG - CSP	Counter DRBG (A6502)		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS 1.3 Salt	Salt used in HKDF command for TLS 1.3 establishment support	8 to 1024 - -	HMAC - CSP			Key derivation
TLS 1.3 Shared Secret Z	Output of ECDH operation during TLS 1.3 session establishment	224/256/384/521 - 112/128/192/256	SP800-56Ar3 - CSP		KAS-ECC Sp800-56Ar3 (A6594)	Key Exchange Key derivation
TLS 1.3 KDK	Output of TLS 1.3 HKDF extract phase. Used as an input to the key expand phase	256/384 - >=256	HMAC - CSP		TLS v1.3 KDF (A6526)	Key Exchange Key derivation
TLS 1.3 DerivedKeyingMaterial	Key Material from the output of the TLS 1.3 HKDF Expand phase	256 to 1024, 128/256 - >=256, 128/256	HMAC,AES - CSP		TLS v1.3 KDF (A6526)	Key Exchange Key derivation
TLS 1.2 Pre-Master Secret	Pre-Master Secret input to the TLS 1.2 SP800-135 KDF.	384,224/256/384/521 - 256,112/128/192/256	AES256, ECDH(P-224,P-256,P-384,P-521) - CSP	Counter DRBG (A6502)	KAS-ECC Sp800-56Ar3 (A6594)	Key Exchange Key derivation
TLS 1.2 Master Secret	The master secret is the output of the TLS 1.2 SP800-135 KDF.	384 - 112 to 256	TLS v1.2 KDF RFC7627 - CSP		TLS v1.2 KDF RFC7627 (A6525)	Key Exchange Key derivation
TLS 1.2 DerivedKeyingMaterial	The key block output from	256 to 1024, 128/256 -	TLS v1.2 KDF RFC7627 - CSP		TLS v1.2 KDF	Key Exchange

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	SP800-135 KDF using the TLS 1.2 Master Secret as input. This material can be used as the TLS 1.2 encryption and integrity key	>=256, 128/256			RFC7627 (A6525)	Key derivation
CMAC FCE	CMAC Key/Keygroup used to compute CMAC using FCE	128 - 128	CMAC - CSP	Counter DRBG (A6502)		FCE-MAC
HMAC FCE	HMAC Key/Keygroup used to compute HMAC using FCE	256 - 256	HMAC - CSP	Counter DRBG (A6502)		FCE-MAC
PUB_ES_ECC	Externally supplied ECC keys	448/512/768/1042/512/256 - 112/128/192/256/128/128	ECC ECDSA (P-224,P-256,P-384,P-521,brainpoolP256r1),EDDSA (Ed25519) - PSP			Verify
PUB_TOPKG_ECC	Transient output associated with private ECC keygen	448/512/768/1042/512/256 - 112/128/192/256/128/128	ECC ECDSA (P-224,P-256,P-384,P-521,brainpoolP256r1),EDDSA (Ed25519) - PSP	ECDSA KeyGen (FIPS186-5) (A6542) EDDSA KeyGen (A6528)		
PUB_ES_ECDH	Externally supplied ECDH keys	448/512/768/1042/512 - 112, 128, 192, 256, 128	ECDH (P-224,P-256,P-384,P-521,brainpoolP256r1) - PSP			Key Exchange
PUB_TOPKG_ECDH	Transient output associated	448/512/768/1042/512 -	ECDH(P-224,P-256,P-384,P-	KAS-ECC Sp800-		Key Exchange

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	with private ECDH keygen	112/128/192/256/128	521,brainpoolP256r1) - PSP	56Ar3 (A6594)		Key derivation
PUB_ES_RSA	Externally supplied for RSA Sign Verify operations only	2046/3072/4096 - 112/128/140	RSASSA-PKCS1-V1_5, RSASSA-PSS - PSP			Verify
PUB_TOPKG_RSA	Transient Output associated with private key gen for RSA Sign Verify operations only.	2048/3072/4096 - 112/128/140	RSASSA-PKCS1-V1_5, RSASSA-PSS - PSP	RSA KeyGen (FIPS186-5) (A6593)		
PUB_ES_Root	Root public keys externally supplied	2048/3072/4096 448/512/768/1042 256 - 112/128/140, 112/128/192/256 128	RSA(2048,3072,4096),ECDSA(P-256,P-384,P-521),EDDSA (Ed25519) - PSP			Verify
PUB_X509_Cert_ES	X.509 Certificate externally supplied	2048/3072/4096 448/512/768/1042 256 - 112/128/140, 112/128/192/256	RSA(2048,3072,4096),ECDSA(P-256,P-384,P-521), EDDSA (Ed25519) - PSP			Verify

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		128				
PUBK_X509	Public key extracted from X.509 Certificate	2048/3072/4096 448/512/768/1042 256 - 112/128/140, 112/128/192/256 128	RSA(2048,3072,4096),ECDSA(P-256,P-384,P-521), EDDSA (Ed25519) - PSP			Verify
DUPK	DevUpdate Public Key	1042 - 256	ECDSA:P-521 - PSP			GCM-ENC

Table 20: SSP Table 1

Note *: The “Proof Key” CSP is only 128-bits security strength for functions that use this key. However, the only service which uses this key (Storage Extension) must be through an Auth session which may be 128 or 256-bit security strength. For a 256-bit session, the exported blob will have 256-bit security strength protection.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
RKEK	Manufacturing-Input	SRAM:Plaintext NVM EEPROM:Plaintext		SRAM Zeroization Master Delete	CTR KEK:Generates
CTR KEK		SRAM:Plaintext		SRAM Zeroization	RKEK:Derived from COK:Wraps COK2:Wraps UAK:Wraps CKAES:Wraps CKGCM:Wraps

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
RPKK		NVM EEPROM:Plaintext SRAM:Plaintext		SRAM Zeroization Master Delete	Proof Key:Derives
Proof Key		SRAM:Plaintext		SRAM Zeroization	RPKK:Derived From CKAES:Wraps CKECDSA:Wraps PUB_ES_ECC:Wraps
COK	Manufacturing-Input	SRAM:Plaintext NVM EEPROM:Encrypted		Master Delete SRAM Zeroization	ASK:Derives
COK2	Auth Session In Bound Auth Session Outbound	SRAM:Plaintext NVM EEPROM:Encrypted		SRAM Zeroization Master Delete	ASK:Derives COK:Written by
UAK	Auth Session In Bound Auth Session Outbound	NVM EEPROM:Encrypted SRAM:Plaintext		SRAM Zeroization Master Delete	ASK:Derives COK:Written by COK2:Written by
ASK		SRAM:Plaintext		SRAM Zeroization	UAK:Derived from COK:Derived from COK2:Derived from
CKAES	Auth Session In Bound Auth Session Outbound	NVM EEPROM:Encrypted SRAM:Plaintext		SRAM Zeroization Master Delete	UAK:Authorized by COK:Authorized by
CKHMAC	Auth Session In Bound Auth Session Outbound	NVM EEPROM:Encrypted SRAM:Plaintext		SRAM Zeroization Master Delete	UAK:Authorized by
CKCMAC	Auth Session In Bound Auth	NVM EEPROM:Encrypted		SRAM Zeroization	UAK:Authorized by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Session Outbound	SRAM:Plaintext		Master Delete	
CKGCM	Auth Session In Bound Auth Session Outbound	NVM EEPROM:Encrypted SRAM:Plaintext		SRAM Zeroization Master Delete	UAK:Authorized by
CKECDSA	Auth Session In Bound Auth Session Outbound	SRAM:Plaintext NVM EEPROM:Encrypted		SRAM Zeroization Master Delete	CKECDSAK:Used With PUB_TOPKG_ECC:Generates
CKECDSAK		SRAM:Plaintext		SRAM Zeroization	CKECDSA:Used with
CKECDH	Auth Session In Bound Auth Session Outbound	NVM EEPROM:Encrypted SRAM:Plaintext		SRAM Zeroization Master Delete	PUB_ES_ECDH:Used with
CKRSA	Auth Session In Bound Auth Session Outbound	NVM EEPROM:Encrypted SRAM:Plaintext		SRAM Zeroization Master Delete	PUB_TOPKG_RSAÃ‚Â : Generates
ECDH Shared Secrets (Z)		SRAM:Plaintext		SRAM Zeroization	CKECDH:Derived from SP800-56Cr2 Salt:Used with KDK:Derives
SP800-56Cr2 Salt	Auth Session In Bound	SRAM:Plaintext		SRAM Zeroization	ECDH Shared Secrets (Z):Used with KDK:Derives
KDK		SRAM:Plaintext		SRAM Zeroization	Derived Key Material:Derives
Derived Key Material	Auth Session Outbound	NVM EEPROM:Encrypted SRAM:Plaintext		SRAM Zeroization Master Delete	CKGCM:Derives CKHMAC:Derives

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
MDUK	Manufacturing-Input	SRAM:Plaintext NVM EEPROM:Plaintext		SRAM Zeroization Master Delete	DevUpdate Key:Derives
DevUpdate Key		SRAM:Plaintext		SRAM Zeroization	COK:Authorized by
Entropy Input String		SRAM:Obfuscated		SRAM Zeroization	DRBG Input Seed:Derives
DRBG Input Seed		SRAM:Plaintext		SRAM Zeroization	DRBG Internal State:Modifies Entropy Input String:Derived from
DRBG Internal State		SRAM:Plaintext		SRAM Zeroization	DRBG Input Seed:Modifies Entropy Input String:Modifies
TLS 1.3 Salt	Auth Session In Bound	SRAM:Plaintext		SRAM Zeroization	TLS 1.3 Shared Secret Z:Used with TLS 1.3 KDK:Derives
TLS 1.3 Shared Secret Z		SRAM:Encrypted		SRAM Zeroization	TLS 1.3 KDK:Derives
TLS 1.3 KDK		SRAM:Plaintext		SRAM Zeroization	TLS 1.3 DerivedKeyingMaterial:Derives
TLS 1.3 DerivedKeying Material	Auth Session Outbound	SRAM:Plaintext NVM EEPROM:Encrypted		SRAM Zeroization Master Delete	CKGCM:Derives CKHMAC:Derives
TLS 1.2 Pre-Master Secret		SRAM:Encrypted		SRAM Zeroization	TLS 1.2 Master Secret:Derives
TLS 1.2 Master Secret	Auth Session In Bound	SRAM:Encrypted		SRAM Zeroization	TLS 1.2 DerivedKeyingMaterial:Derives
TLS 1.2 DerivedKeying Material	Auth Session Outbound	SRAM:Encrypted		SRAM Zeroization	CKGCM:Derives CKHMAC:Derives
CMAC FCE	Auth Session In Bound	NVM EEPROM:Encrypted		SRAM Zeroization	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Auth Session Outbound	SRAM:Plaintext		Master Delete	
HMAC FCE	Auth Session In Bound Auth Session Outbound	NVM EEPROM:Encrypted SRAM:Plaintext		SRAM Zeroization Master Delete	
PUB_ES_ECC	Auth Session Outbound Auth Session In Bound	SRAM:Plaintext NVM EEPROM:Plaintext		SRAM Zeroization	UAK:Authorized by
PUB_TOPKG_ECC	Auth Session Outbound	SRAM:Plaintext		SRAM Zeroization	CKECDSA:Generated by
PUB_ES_ECDH	Auth Session In Bound	SRAM:Plaintext		SRAM Zeroization	CKECDH:Used with
PUB_TOPKG_ECDH	Auth Session Outbound	SRAM:Plaintext		SRAM Zeroization	CKECDH:Generated by
PUB_ES_RSA	Auth Session In Bound Auth Session Outbound	SRAM:Plaintext NVM EEPROM:Plaintext		SRAM Zeroization	UAK:Authorized by
PUB_TOPKG_RSA	Auth Session Outbound	SRAM:Plaintext		SRAM Zeroization	CKRSA:Generated by
PUB_ES_Root	Auth Session In Bound Auth Session Outbound	SRAM:Plaintext NVM EEPROM:Plaintext		SRAM Zeroization	PUB_X509_Cert_ES:Validates PUBK_X509:Validates
PUB_X509_Cert_ES	Auth Session In Bound Auth Session Outbound	SRAM:Plaintext NVM EEPROM:Plaintext		SRAM Zeroization	PUB_ES_Root:Validated by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
PUBK_X509	Auth Session Outbound	SRAM:Plaintext NVM EEPROM:Plaintext		SRAM Zeroization	PUB_ES_Root:Validated by
DUPK	Manufacturing-Input	SRAM:Plaintext NVM EEPROM:Plaintext		SRAM Zeroization Master Delete	COK:Authorized by

Table 21: SSP Table 2

Note: All public keys (PUB_xxxx) in the SSP Table 2 are protected by an integrity CRC-16 validation. Per FIPS 140-3 IG 9.6.A these keys are not zeroized.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
NVM Patch Code Integrity	Checksum match	CRC-16	SW/FW Integrity	State: OPERATIONAL or ERROR	CRC 16-bit Validation of NVM executable code.
NVM Configuration Integrity	Checksum match	CRC-16	Critical Function	State: OPERATIONAL or ERROR	CRC 16-bit Validation of NVM configuration areas

Table 22: Pre-Operational Self-Tests

Order of Execution of POST Tests:

1. NVM Patch Code Integrity Test (CRC-16)
2. NVM Configuration Integrity Test (CRC-16)

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ACE NRBG RCT	Detect Entropy < 50%	Repetition Count Test	CAST	State: ERROR	SP800-90B Repetition Count Test	Automatically on power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ACE NRBG APT1	Detect Entropy < 50%. Window=1k samples	Adaptive Proportion Test	CAST	State: ERROR	SP800-90B Adaptive Proportion Test	Automatically on power up
ACE NRBG APT2	Detect Entropy < 50%, window=256 samples	Adaptive Proportion Test	CAST	State: ERROR	SP800-90B Adaptive Proportion Test	Automatically on power up
Counter DRBG (A6502)	Key Length: 256-bits, Derivation Function	KAT	CAST	State: OPERATIONAL or ERROR	AES-256 Counter Mode DRBG	Automatically on power up and On Demand
HMAC-SHA2-512 (A6488)	Hash: 512-bits, Key Length: 512-bits	KAT	CAST	State: OPERATIONAL or ERROR	MAC Generation	Before first use and On Demand
HMAC-SHA2-256 (A6488)	Hash: 256-bits, Key Length: 256-bits	KAT	CAST	State: OPERATIONAL or ERROR	MAC Generation	Automatically on power up and On Demand
AES-CMAC Generation (A6562)	Key Length: 128-bits	KAT	CAST	State: OPERATIONAL or ERROR	Generation	Before first use and On Demand
AES-CMAC Verification (A6562)	Key Length: 128-bits	KAT	CAST	State: OPERATIONAL or ERROR	Verification	Before first use and On Demand
AES-GCM Encrypt (A6521)	AES GCM KAT, Key Length: 128-bits	KAT	CAST	State: OPERATIONAL or ERROR	Encrypt	Automatically on power up and On Demand
AES-GCM Decrypt (A6521)	AES GCM KAT, Key Length: 128-bits	KAT	CAST	State: OPERATIONAL or ERROR	Decrypt	Automatically on power up and On Demand
ECDSA SigGen (FIPS186-5) (A6522)	Curve: P256	KAT	CAST	State: OPERATIONAL or ERROR	SigGen	Before first use and On Demand

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-5) (A6522)	Curve: P256	KAT	CAST	State: OPERATIONAL or ERROR	SigVer	Before first use and On Demand
FW Load Test (AES-GCM A6521)	AES GCM KAT, Key Length: 128-bits	KAT	SW/FW Load	State: RESET or new FW version reported	AES-GCM authenticated decryption of firmware	On Demand
KAS-ECC Sp800-56Ar3 (A6594)	KAS KAT, Curve: P256, Ephemeral Unified, Initiator, Responder, Two Step KDF	KAT	CAST	State: OPERATIONAL or ERROR	Key Agreement	Before first use and On Demand
EDDSA SigGen (A6523)	Curve: ED-25519, pure functionality, sign pre-hashed messages	KAT	CAST	State: OPERATIONAL or ERROR	SigGen	Before first use and On Demand
EDDSA SigVer (A6523)	Curve: ED-25519, pure functionality, sign pre-hashed messages	KAT	CAST	State: OPERATIONAL or ERROR	SigVer	Before first use and On Demand
RSA SigGen (FIPS186-5) (A6527)	Key Length: 2048, PKCS#1 v1.5. SHA-256	KAT	CAST	State: OPERATIONAL or ERROR	SigGen	Before first use and On Demand
RSA SigVer (FIPS186-5) (A6527)	Key Length: 2048, PKCS#1 v1.5. SHA-256	KAT	CAST	State: OPERATIONAL or ERROR	SigVer	Before first use and On Demand
KDF SP800-108 (A6524)	Mode: Counter, MAC: HMAC-SHA2-256	KAT	CAST	State: OPERATIONAL or ERROR	Key Derivation	Before first use and On Demand
TLS v1.2 KDF	MAC: HMAC-SHA2-256	KAT	CAST	State: OPERATIONAL or ERROR	TLS 1.2 Key Derivation	Before first use and On Demand

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RFC7627 (A6525)						
TLS v1.3 KDF (A6526)	MAC: HMAC-SHA2-256	KAT	CAST	State: OPERATIONAL or ERROR	TLS 1.3 Key Derivation	Before first use and On Demand
ECDSA KeyGen PCT (A6542)	Curve size: 224, 256, 384, 521	PCT	PCT	State: OPERATIONAL or ERROR	KeyGen	Automatic on key generation
EDDSA KeyGen PCT (A6528)	Curve: ED-25519	PCT	PCT	State: OPERATIONAL or ERROR	KeyGen	Automatic on key generation
KAS-ECC Sp800-56Ar3 PCT (A6594)	Curve size: 224, 256, 384, 521	PCT	PCT	State: OPERATIONAL or ERROR	KeyGen	Automatic on key generation
RSA KeyGen PCT (A6593)	Key size: 2048,3072,4096	PCT	PCT	State: OPERATIONAL or ERROR	KeyGen	Automatic on key generation
AES-CMAC (A874)	Key Length: 128 bits	KAT	CAST	State: OPERATIONAL or ERROR	MAC Generation	Before first use and On Demand
HMAC-SHA2-256 (A853)	Hash: 256-bits, Key Length: 256-bits	KAT	CAST	State: OPERATIONAL or ERROR	MAC Generation	Before first use and On Demand

Table 23: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
NVM Patch Code Integrity	CRC-16	SW/FW Integrity	Automatically on power up	Power cycle
NVM Configuration Integrity	CRC-16	Critical Function	Automatically on power up, Reset or Wake	Power cycle, Reset or Wake

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ACE NRBG RCT	Repetition Count Test	CAST	Continuous	Power cycle
ACE NRBG APT1	Adaptive Proportion Test	CAST	Continuous	Power cycle
ACE NRBG APT2	Adaptive Proportion Test	CAST	Continuous	Power cycle
Counter DRBG (A6502)	KAT	CAST	Power cycle or On Demand	Power cycle or Self_test command
HMAC-SHA2-512 (A6488)	KAT	CAST	On Demand	Self_Test command
HMAC-SHA2-256 (A6488)	KAT	CAST	Power cycle or On Demand	Power cycle or Self_test command
AES-CMAC Generation (A6562)	KAT	CAST	On Demand	Self_Test command
AES-CMAC Verification (A6562)	KAT	CAST	On Demand	Self_Test command
AES-GCM Encrypt (A6521)	KAT	CAST	Power cycle or On Demand	Power cycle or Self_Test command
AES-GCM Decrypt (A6521)	KAT	CAST	Power cycle or On Demand	Power cycle or Self_Test command
ECDSA SigGen (FIPS186-5) (A6522)	KAT	CAST	On Demand	Self_Test command
ECDSA SigVer (FIPS186-5) (A6522)	KAT	CAST	On Demand	Self_Test command
FW Load Test (AES-GCM A6521)	KAT	SW/FW Load	On Demand	Dev_Update command
KAS-ECC Sp800-56Ar3 (A6594)	KAT	CAST	On Demand	Self_Test command
EDDSA SigGen (A6523)	KAT	CAST	On Demand	Self_Test command
EDDSA SigVer (A6523)	KAT	CAST	On Demand	Self_Test command
RSA SigGen (FIPS186-5) (A6527)	KAT	CAST	On Demand	Self_Test command

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-5) (A6527)	KAT	CAST	On Demand	Self_Test command
KDF SP800-108 (A6524)	KAT	CAST	On Demand	Self_Test command
TLS v1.2 KDF RFC7627 (A6525)	KAT	CAST	On Demand	Self_Test command
TLS v1.3 KDF (A6526)	KAT	CAST	On Demand	Self_Test command
ECDSA KeyGen PCT (A6542)	PCT	PCT	On Usage	Automatic on key generation
EDDSA KeyGen PCT (A6528)	PCT	PCT	On Usage	Automatic on key generation
KAS-ECC Sp800-56Ar3 PCT (A6594)	PCT	PCT	On Usage	Automatic on key generation
RSA KeyGen PCT (A6593)	PCT	PCT	On Usage	Automatic on key generation
AES-CMAC (A874)	KAT	CAST	On Demand	Self_Test command
HMAC-SHA2-256 (A853)	KAT	CAST	On Demand	Self_Test command

Table 25: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
ERROR	Module has failed a Self-Test. FIPS approved services are not provided by the module when it is in this state and data output is inhibited, except for status data.	Pre-Operational Self-Tests, Conditional Self-Tests, or NRBG Health Test failure.	The module will clear this ERROR state on a RESET pin assertion, wake reset or power-up reset event.	Show Status (Device Information and Status service)

Table 26: Error States

Upon encountering a self-test failure state, the TA101 module will remain in this error state until an error recovery is attempted. While the module is in the error state, data output (except for status data) is inhibited by the module. The module will not allow any operations or commands other than Show Version - Status (Device Information and Status service), Power Management, and Run Self-tests (Cryptographic Self-Test service) to be executed.

Recovery, the module can only clear the failure state on a RESET pin assertion, wake reset or power-up reset event, due to configuration parameter chip_option.Reset_Fail=0x01. The operator may execute the Show Version - Status command to check if the model is ready to receive commands.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Crypto Officer role is established during the Microchip Manufacturing process and the device locked in the FIPS 140-3 compliant approved mode of operation.

There is only one combination of configuration bits that allow the device to be in the FIPS 140-3 compliant approve mode of operation. These configuration bits are detailed below. Other configuration bits within the device have no impact on the approved mode of operation and are not detailed here. See the product datasheet for further details about these configuration bits.

To invoke the approved mode of operation the module must be configured with the following:

Minimum Compliance configuration:

1. Set self_test_config.Power_Up = 0x0000 0000
2. Set self_test_config.Wake = 0xXXXX XXXX
3. Set self_test_config.On_Demand = 0xD738 A000
4. Set self_test_config.Failure_Clear = 0xXXXX XXXX
   The device can only clear the failure state on a RESET pin assertion, wake reset or power-up reset event, due to chip_option.Reset_Fail=0x1.

Firmware Update configuration:

1. Set Device_Update.Downgrade_OK = 0x0
2. Set Device_Update.Erase_OK = 0x0
3. Set Device_Update.Power_up_check = 0x1
4. Set Device_Update.Auth_Update = 0x1
5. Set Device_Update.Update_Key = KKK (KKK=ID of Crypto Officer Key)

Chip Options configuration:

1. Set chip_option.Compliance = 0x1
2. Set chip_option.Reset_Fail =0x1
3. Set chip_option.HDCP_Enable =0x0
4. Set chip_option.ECBD_Disable =0x1
5. Set chip_option.SECP256k1_Disable =0x1
6. Set chip_option.X25519_Disable =0x1
7. 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.Config_Test = 0x1
2. Set compliance_option.Update_Test = 0x1
3. Set compliance_option.Public_Auth = 0x1
4. Set compliance_option.RW_SHA_CTX = 0x0

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

Master delete configuration:

1. Set Master_Delete.Enable = 0x1
2. Set Master_Delete.Auth_Key = KKK (KKK=ID of Crypto Officer Key)

Secure Boot Configuration:

1. Mode = 2, Full Stored, is not permitted
2. Mode = 3, Partial, only permitted when Auth_boot = 1

Global Export configuration:

3. Set Global_Export.Forbid = 0x0
4. Set Global_Export.Auth_Req = 0x1
5. 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.

These configuration bits, along with other general configuration bits defined by the end user, are written and locked at the Microchip Manufacturing site during the production test. 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.

11.2 Non-Administrator Guidance

Non-administrative guidance describes the security functions of the cryptographic module along with instructions, guidelines, and warnings for the secure use of the module.

1. The full list of permissible operator approved security services is defined in the above services table in this security policy.
2. Physical ports, and logical interfaces: The operator has access to all the modules physical ports and logical interfaces.

General TA101 usage information can be obtained from the public Microchip.com website.

1. See summary data sheet "TA101 CryptoAutomotive Summary Data Sheet DS40002529".
2. See application note “TA101 FIPS 140-3 Compliance Guidance AN5825“.

11.3 Design and Rules

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

All security rules are enforced by the module when configured in FIPS 140-3 approved mode of operation. The device does not support a non-approved mode.

1. The cryptographic module does not support a non-compliant state or a non-approved mode. The cryptographic module is shipped from manufacturing in the approved mode of operation. During manufacturing, the cryptographic module is provisioned with the necessary COK (T=0) and COK2 authentication data required by the Cryptographic Officer (CO). The CO can update COK2 in the field as required. In such a case when updating the COK2 or generating a new COK2, it must always be created in the special handle range of 80F0 – 80FF

2. COK Key properties configured at Microchip manufacturing provisioning contain properties that the key can never be modified. This key may be zeroized by the Zeroize service triggered by the Cryptographic Officer.
3. When performing the Secure Firmware Update service, the operator shall
    a. Authenticate as the CO.
    b. Ensure that the Power_up_check bit is set.
4. When performing the Zeroize service, the operator shall
    a. Authenticate as the CO.
5. Public keys shall not be entered or output in plaintext. These keys shall only be entered or output using AES GCM ASK.
6. Exporting public keys using AES GCM ASK shall only be performed inside an Auth Session.
7. RSA and ECC keys shall only be generated using SP800-90A DRBG (using SP800-56A is disallowed).
8. The GCM IV is generated using an Approved DRBG using a 96-bit seed generated inside the module's cryptographic boundary. The IV is always regenerated after power is lost.
9. 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.
10. The module supports a maximum of simultaneous 2 Auth Sessions (i.e. a maximum of two concurrent operators).
11. The cryptographic module does not provide any service/interface to output authentication data in plaintext.
12. Any symmetric or private key that has "Read_Perm", "Usage_Perm" or "Write_Perm" set to "Always" is prohibited.
13. Authorization sessions must be run using the GCM algorithm and the key must be derived using the RNG. For this reason, values other than 3, 4 and 7 are prohibited for the Session_Use" field within the symmetric key properties field for those keys intended to initiate an authorization session.
14. Either signature or key agreement, but not both, is allowed within the private key property fields of "Sign_Use" and "Agree_Use". "Sign_Use" equal to `b01 is not allowed as a given key and must not be allowed to sign both internally and externally generated digests.
15. AES ECB encryption/decryption through the AES command is disallowed.
16. Generally, the mode of AES keys is enforced. AES keys where the mode is set to GCM can be used only for GCM operations and similarly for the CMAC mode.
17. Command RSA_ENC is disabled. Any use of RSA-1024, RSA-2048, RSA-3072, RSA-4096 encrypt/decrypt is prohibited.
18. For RSA-3072, exponents of 3 are prohibited for all operations including Verify.
19. Any read or write of a symmetric or private key, if allowed at all, must run within an authorization session encrypted using GCM.
20. The functions SHA-256 KDF, HDCP, ECBD, SECP256k1 and X25519 are disabled.
21. Sign/Verify commands enforce atomic message digest creation with the Sign/Verify operation when configuration bits are properly defined.
22. The Compliance_Option configuration bit Public_Auth must be set, while the RW_SHA_CTX bit must not be set.
23. The Chip_Options configuration bit Sign_Internal_Auth must be set.

24. If Public_Auth is set, all portions of the X.509 certificate sent to the Manage_Cert command when validating a certificate must be authorized using the parent key's authorization key. The Parent_Handle will not be ignored for any portion.
25. If Public_Auth is set, the public key cannot be passed to the TA101 in the input buffer for the Verify commands.
26. The ECDH command shall only be performed inside an Authorization Session. ECDH is permitted only if the output is an ephemeral key.
27. Key Generation shall only be performed inside an Authorization Session.

11.4 Administrator Guidance

The security parameters, physical ports, and logical interfaces for the Administrator (CO (Crypto Officer)) are defined via this Security Policy.

The Crypto Officer role is established during the Microchip Manufacturing process when the TA101 device is locked in the FIPS 140-3 compliant approved mode of operation and will have the below unique capabilities. The full list of permissible services by the CO is defined in the above services table in this security policy.

Service "SSP Element Creation": Create other crypto officer keys.
Service "SSP Element Creation": Create USER (CO2) roles.
Service "Secure Firmware Update": Firmware update is limited to the crypto officer.
Service "Zeroize": Device sanitization is limited to the crypto officer.

Physical ports, and logical interfaces: The Crypto Officer has access to all the modules physical ports and logical interfaces.

11.5 Maintenance Requirements

The Module does not support a maintenance interface, maintenance mode, nor a maintenance role.

11.6 End of Life

If the Crypto Officer would like to render the Module as no longer operable (end of life), the Crypto Officer must securely sanitize the Module using the "Zeroize" service during an authentication session. The device will automatically perform a power-cycle at the end of the service. (See the application note "TA101 FIPS 140-3 Compliance Guidance AN5825" for further End of Life options).

During this process it is not possible to extract critical security keys or data information from the device. Once sanitized the device will not be capable of being restored to its original or an alternate provisioning configuration that could allow a system to restore its functionality.

Note that this process will cause the module to no longer function in its application.

12 Mitigation of Other Attacks

12.1 Attack List

General TA101 information can be obtained from the public Microchip.com website.

- See summary data sheet "TA101 CryptoAutomotive Summary Data Sheet DS40002529".
  - Section 5: The TA101 device includes protection against both active (invasive) and passive (non-invasive) attacks on the certificates, private and symmetric keys stored within the device. Specific hardware and firmware elements are included to prevent environmental (voltage, temperature and frequency) attacks, emissions attacks, fault attacks, physical attacks, cloning and many other attack methodologies. All internal memory for private/symmetric keys or other secret data is encrypted.

12.2 Mitigation Effectiveness

The effectiveness of the countermeasures within the TA101 device to mitigate attacks has been evaluated by a third-party laboratory. Contact Microchip for further details about the mitigation effectiveness.

13. 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
EDDSA	Edwards-curve Digital Signature Algorithm
ESV	Entropy Source Validation
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
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

Exhibit 13-1 Specification of Acronyms and their Descriptions