Caliptra Root of Trust for Measurement (RTM)

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document defines the Non-Proprietary Security Policy for the *Caliptra Root of Trust for Measurement (RTM)* module, hereafter denoted the Module.

The Module is a limited operational environment under the FIPS 140-3 definitions. The Module includes a firmware load function. New firmware versions within the scope of this validation must be validated through the CMVP; any other firmware loaded into the Module is out of the scope of this validation and requires a separate FIPS 140-3 validation.

The Module meets FIPS 140-3 overall Level 1 requirements, with security levels as specified in Section 1.2.

1.2 Security Levels

Section	Security Level
1	1
2	1
3	1
4	1
5	1
6	N/A
7	1
8	N/A
9	1
10	1
11	3
12	1

Table 1: Security Levels

The Module is validated to Level 1 overall with *Life-Cycle Assurance* (Section 7.11) Level 3 to allow the Module to be embedded into or bound with another validated module seeking Level 2 or 3 overall.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Module is a dedicated security controller subsystem of the <vendor / module specific description>. The Module is a sub-chip subsystem (single-chip embodiment) that provides a hardware root of trust for measurement and identity.

The Module's formal name is < vendor / module specific name>. The Module is available in the configurations shown in Table 2.

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

Module Type: Hardware

Module Embodiment: SingleChip

Module Characteristics: SubChip

Cryptographic Boundary:

The Module complies with all FIPS 140-3 IG 2.3.B *Sub-Chip Cryptographic Subsystems* requirements. The cryptographic boundary is the set of components within the dashed red line of Figure 1, inclusive of all hardware and firmware components that comprise the Module as a sub-chip subsystem.

The Module boots from an internal ROM but requires a firmware container to be loaded into RAM: during the initialization peri od, the loaded firmware is verified with an approved authentication method in accordance with firmware load test requirements.

The hardware module interface (HMI) is defined at the sub-chip cryptographic subsystem boundary.

The pre-operational approved integrity test is performed over all firmware components within the cryptographic boundary.

Private and secret keys cross logical and physical boundaries only in the form of <TBD>, meeting FIPS 140-3 IG 9.5.A and D.G requirements.

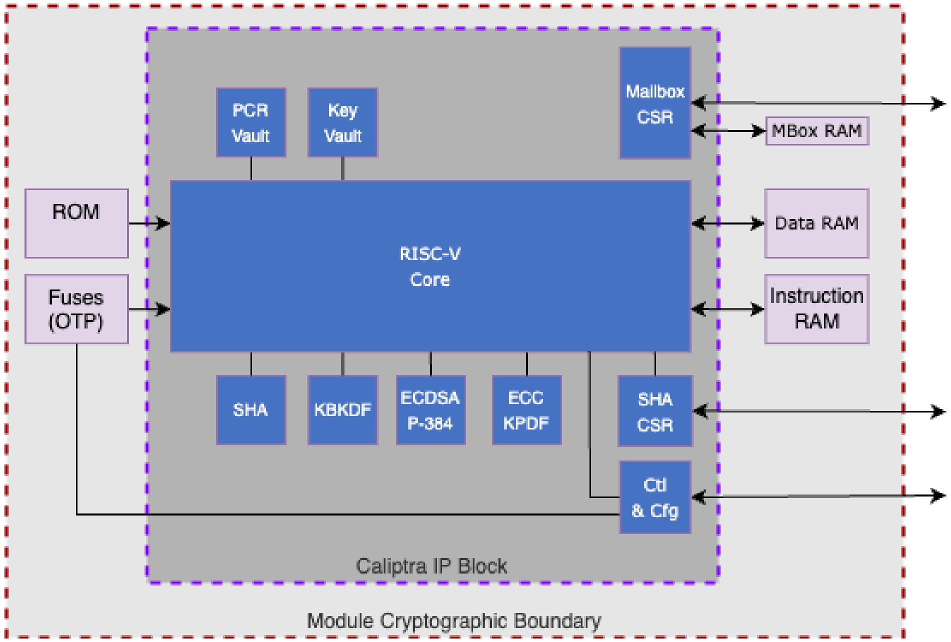

Figure 1: Block Diagram

Tested Operational Environment's Physical Perimeter (TOEPP):

<Specify TOEPP>

The physical form of the Module is shown in Figure 2.

Figure 2: Module Physical Form

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
TBD	TBD	TBD	TBD	TBD

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

N/A for this module.

2.4 Modes of Operation

Modes List and Description:

Table Name	Description	Type	Status Indicator
Nominal	The module's normal operating mode.	Approved	fips_status:0

Table 3: Modes List and Description

The Module as defined above will always be in an Approved mode of operation. No configuration is necessary for the Module to operate and remain in the Approved mode. The Module design corresponds to the Module security rules (see Section 11.4).

The conditions for using the Module in the Approved mode of operation are:

1. Installation of the Module as described in Section 11.1 results in the settings described below, which are required for operation in the Approved mode:
   a. <TBD>.
2. The Module is a functional block integrated into an FPGA or SoC. The integrator is responsible for:
   b. <TBD>.

Mode Change Instructions and Status [O]:

<Text>

2.5 Algorithms

Approved Algorithms:

Digest

Algorithm	CAVP Cert	Properties	Reference
SHA2-384	A9997	-	FIPS 180-4
SHA2-512	A9997	-	FIPS 180-4

Table 4: Approved Algorithms - Digest

ECC KPDF

Algorithm	CAVP Cert	Properties	Reference
SHA2-384	A9998	-	FIPS 180-4
HMAC-SHA2-384	A9998	-	FIPS 198-1
HMAC DRBG	A9998	-	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A9998	-	FIPS 186-5
KDF SP800-108	A9998	-	SP 800-108 Rev. 1

Table 5: Approved Algorithms - ECC KPDF

Identity and Authentication

Algorithm	CAVP Cert	Properties	Reference
SHA2-256	A9999	-	FIPS 180-4
Deterministic ECDSA SigGen (FIPS186-5)	A9999	-	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A9999	-	FIPS 186-5
LMS SigVer	A9999	-	SP 800-208

Table 6: Approved Algorithms - Identity and Authentication

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG Section 5		Caliptra Vendor DCSoC HW	NIST, SP 800-133 Rev. 2

Table 7: 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
AES	Not CAVP listed, not self-tested	Obfuscation.
SHA-1	Not CAVP listed	Certificate identifiers.

Table 8: Non-Approved, Allowed Algorithms with No Security Claimed

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Digest	SHA	External SHA accelerator - digest calculation.		SHA2-384 SHA2-512
ECC KPDF	AsymKeyPair-KeyGen CKG DRBG	Deterministic ECC Key Generation (NIST CTG Reviewed)		SHA2-384 HMAC-SHA2-384 HMAC DRBG ECDSA KeyGen (FIPS186-5) CKG Section 5
KBKDF	KBKDF MAC SHA	HMAC CTR SP 800-108 KBKDF.		SHA2-384 HMAC-SHA2-384 KDF SP800-108
Other-Mfr	Other - Externally generated SSPs	Placeholder for externally generated SSPs		Other - Externally generated SSPs
SigGen	DigSig-SigGen	Deterministic ECDSA P-384, SHA2-384 signature generation		Deterministic ECDSA SigGen (FIPS186-5) SHA2-384
SigVer	DigSig-SigVer	ECC or LMS Signature Verification		SHA2-256 SHA2-384 ECDSA SigVer (FIPS186-5) LMS SigVer

Table 9: Security Function Implementations

2.7 Algorithm Specific Information

<Text>

2.8 RBG and Entropy

N/A for this module.

2.9 Key Generation

The Module:

- Does not provide symmetric key generation.
- Produces asymmetric keys in accordance with …
- Supports symmetric key derivation in accordance with SP 800-133r2 Section 6.2, using the approved and CAVP listed KDF algorithms.

2.10 Key Establishment

<Text>

2.11 Industry Protocols

N/A for this module.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
SoC power	Power	None
SoC Control and Status Wireset	Control Input Status Output	No data; placeholder for control (e.g. CLOCK) and status (e.g. READY) wires.
Mailbox	Control Input Data Input Data Output Status Output	Caliptra mailbox commands and responses.
SHA Engine	Control Input Data Input Data Output Status Output	Input message; output digest.
Ctl & Cfg	Control Input Status Output	Memory mapped access to control and configuration registers, status output.

Table 10: Ports and Interfaces

The Control Output interface is not applicable, as the module does not control other components.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO	Role	CO	

Table 11: Roles

The Module supports the mandatory Cryptographic Officer (CO) operational role only (implicitly identified) and does not support a maintenance role or a bypass capability. The CO role is assumed by meeting the conditions of Section 11.2 of this document and in associated Guidance documentation.

4.3 Approved Services

SSP Access indicators:

- G (Generate): The Module generates or derives the SSP.
- R (Read): The SSP is read from the Module (e.g., the SSP is output).
- W (Write): The SSP is updated, imported, or written to the Module.
- E (Execute): The Module uses the SSP in performing a cryptographic operation.
- Z (Zeroize): The Module zeroizes the SSP.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Digest	Calculate a digest using external SHA accelerator	sha_csr_status:0	SHA CSR inputs	SHA CSR outputs	Digest	
Firmware Load	Load and authenticate Caliptra FW image	fips_status:0	Mailbox command frame	Mailbox response frame	SigVer	CO - FW_AK_ECC: E - FW_AK_LMS: E
Identity Management	Reconstruct or obtain device identities in certificate or key formats.	fips_status:0	Mailbox command frame	Mailbox response frame	ECC KPDF KBKDF Other-Mfr SigGen SigVer	CO - UDS: E - FE: E - IDEVID_Priv: G,E - IDEVID_Pub: G,R,W - CDI_n: G,E - LDEVID_Priv: G,E - LDEVID_Pub: G,W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- ALIASn_Priv: G,E - ALIASn_Pub: G,W
Measurement	Manage device measurements.	fips_status:0	Mailbox command frame	Mailbox response frame	Digest SigGen SigVer	CO - CDI_n: G,E - ALIASn_Priv: G,E - ALIASn_Pub: G,W
Sanitize	Sanitize Caliptra SSPs	fips_status:0	Mailbox command frame	Mailbox response frame		CO - UDS: Z - MFG_n_CA_Pub: Z
Self-test	Pre-operational self-test via module HMI	fips_status:0	Mailbox command frame	Mailbox response frame	Digest SigVer	CO - FW_AK_ECC: E - FW_AK_LMS: E
Shutdown	Zeroize Caliptra SSPs	fips_status:0	Mailbox command frame	Mailbox response frame		CO - ALIASn_Priv: Z - ALIASn_Pub: Z - CDI_n: Z - ECC_KPDF_DRBG_Key: Z - ECC_KPDF_DRBG_V: Z - IDEVID_Pub: Z - IDEVID_Pub: Z - LDEVID_Priv: Z - LDEVID_Pub: Z
Utility	Information retrieval and administrative commands	fips_status:0	Mailbox command frame	Mailbox response frame		
Verify	Verify a digital signature	fips_status:0	Mailbox command frame	Mailbox response frame	Digest SigVer	CO - ALIASn_Pub: E - IDEVID_Pub: E - LDEVID_Pub: E
Version	Report module name, version and status	fips_status:0	Mailbox command frame	Mailbox response frame		

Table 12: Approved Services

Command frame refers to the mailbox input registers and the associated data <…>

Result frame refers to the mailbox output registers and the associated data <…>

Each *command frame* and *result frame* includes a simple checksum value, permitting the recipient to verify parameter integrity.

Services are only operational in the running state. Any attempts to access services in any other state will result in an error being returned. If the integrity test or any CAST fails, then any attempt to access any service will result in an error being returned. The Module conforms to FIPS 140-3 IG 2.4.C *Approved Security Service Indicator*, similar to example 2. Each service provides context sensitive status responses as described in Caliptra online documentation; generally, functions of return type int return the value 1 for success with other error codes as appropriate for the call.

The <*FIPS_NAME_VERSION*> service response provides the means to confirm the Table 2 Module name and version information. These parameters, along with the Module's internal indicators of the security-check and conditional-errors settings, are used to confirm the Module is the validated Module operating in the Approved mode with only Approved security services.

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

<Text>

5 Software/Firmware Security

5.1 Integrity Techniques

The Module uses ECDSA signature verification (P-384, SHA2-384) as the firmware integrity method.

5.2 Initiate on Demand

The operator can initiate the integrity test on demand by invoking the FIPS_RUN_PO_TEST service.

5.3 Open-Source Parameters [O]

<Text>

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Vendor specific	Vendor specific	Vendor specific

Table 13: Mechanisms and Actions Required

The Module is a single-chip embodiment that meets commercial-grade specifications for power, temperature, reliability, and shock/vibration. The Module is packaged in standard integrated circuit packaging that provides protection from probing and direct visual observation of circuit detail in the visible spectrum, as well as passivation.

8 Non-Invasive Security

N/A for this module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
C	Code image	Dynamic
D	DER certificate	Dynamic
F	Fuse memory	Static
H	Hardware structure	Dynamic
R	RAM	Dynamic

Table 14: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
C	Code image provider	Code image storage	Plaintext	Automated	Electronic	
I	Calling process	Mailbox command input	Plaintext	Automated	Electronic	
M	Entry at manufacture (TBD)	OTP	Plaintext	Automated	Electronic	
O	Mailbox command output	Calling process	Plaintext	Automated	Electronic	

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
F	Fuse memory sanitization (overwrite with ones)	Fuse sanitization	Shutdown command
S	Shutdown (zeroization) service	Shutdown zeroization	Shutdown command
Z	Zeroized on context change	Context change zeroization	Command that changes context or layer

Table 16: SSP Zeroization Methods

Keys used for CASTs and the temporary value used in the integrity test are not SSPs; however, the latter is deleted after use as required by AS05.10.

Zeroization Methods and Associated Rationales

Zeroing on Object Destruction

<Description>

Hardware Register Zeroing (Power Cycle)

<Description>

Fuse SSP Revocation and Zeroing

Key manifest PK hashes permit 4 ECC and 32 LMS variations, each of which may be revoked in turn. A single owner PK is supported for both ECC and LMS. Revocation status is maintained by a 4-bit one-hot revocation mask in OTP.

The revocation of a cryptographic key or an associated hash results in associated Fuse storage being zeroed.

Since by default, unprogrammed Fuse bits are read as '0b', zeroed in this context requires that all zero Fuse bits in a field be programmed to '1b'; Fuse bits already programmed to '1b' must never be attempted to be programmed to '1b'.

Zeroing a Fuse field is summarized as:

1. Update the associated revoked bit implemented in Fuse.
2. Read the current Fuse field that requires zeroization.
3. XOR the read field with a value of all 1s that is equivalent in length to the read field.
4. Program the Fuse field with the XORed value.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ALIASn_Priv	ALIASn (FMC, RT) ECC Key Pair (private)	384 - 192	P-384 - CSP	ECC KPDF		SigGen

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ALIASn_Pub	LDEVID ECC Key Pair (public)	384 - 192	P-384 - PSP	ECC KPDF		SigGen SigVer
CDI_n	Device Compound Identifier (LDEVID, FMC, RT chain)	384 - 256	DECC_SEED - CSP	KBKDF		KBKDF ECC KPDF
ECC_KPDF_DRBG_Key	ECC KPDF HMAC DRBG working state: Key.	384 - 256	HMAC_DRBG_Key - CSP	ECC KPDF		ECC KPDF
ECC_KPDF_DRBG_V	ECC_KPDF_HMAC DRBG working state: V.	384 - 256	HMAC_DRBG_V - CSP	ECC KPDF		ECC KPDF
FE	Field Entropy	384 - 256	DECC_SEED - CSP	Other-Mfr		KBKDF ECC KPDF
FW_AK_ECC	ECC Firmware authentication (signature verification) key.	384 - 192	P-384 - PSP	Other-Mfr		SigVer
FW_AK_LMS	LMS Firmware authentication (signature verification) key.	tbd - 256	LMS_tbd - PSP	Other-Mfr		SigVer
IDEVID_Priv	IDEVID ECC Key Pair (private)	384 - 192	P-384 - CSP	ECC KPDF		SigGen
IDEVID_Pub	IDEVID ECC Key Pair (public)	384 - 192	P-384 - PSP	ECC KPDF		SigGen
LDEVID_Priv	LDEVID ECC Key Pair (private)	384 - 192	P-384 - CSP	ECC KPDF		SigGen
LDEVID_Pub	LDEVID ECC Key Pair (public)	384 - 192	P-384 - PSP	ECC KPDF		SigGen
MFG_n_CA_Pub	Manufacturing certificate (ROOT, SUB) public key	384 - 192	P-384 - PSP	Other-Mfr		SigVer
UDS	Unique Device Secret	384 - 256	DECC_SEED - CSP	Other-Mfr		KBKDF ECC KPDF

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
ALIASn_Priv	I	R:Plaintext	Layer uptime (max)	S	ALIASn_Pub:Paired With
ALIASn_Pub	I O	R:Plaintext	Device uptime (max)	S	ALIASn_Priv:Paired With
CDI_n		R:Plaintext	Device uptime (max)	Z	UDS:CDI_LDEVID Derived from CDI_n:CDI_LDEVID Derives CDI_FMC CDI_n:CDI_FMC Derives CDI_RTn
ECC_KPDF_DRBG_Key		H:Plaintext	Device uptime (max)	Z	ECC_KPDF_DRBG_V:Used With UDS:Derived From CDI_n:Derived From
ECC_KPDF_DRBG_V		H:Plaintext	Device uptime (max)	S	ECC_KPDF_DRBG_Key:Used With ECC_KPDF_DRBG_Seed:Generated From
FE	M	F:Obfuscated R:Obfuscated	Device lifetime	F	CDI_n:Derives LDevId:Derives
FW_AK_ECC	C	C:Plaintext	Device lifetime	F	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
FW_AK_LMS	C	C:Plaintext	Device lifetime	F	
IDEVID_Priv		H:Plaintext	Layer lifetime	S	IDEVID_Pub:Paired With
IDEVID_Pub	O	R:Plaintext	Device lifetime	Z	IDEVID_Pub:Paired With
LDEVID_Priv		H:Plaintext	Layer lifetime	S	LDEVID_Pub:Paired With
LDEVID_Pub	O	R:Plaintext	Device lifetime	Z	LDEVID_Pub:Paired With
MFG_n_CA_Pub	M	F:Plaintext	Device lifetime	F	MFG_n_CA_Pub:SUB Verified By ROOT MFG_n_CA_Pub:ROOT Verifies SUB IDEVID_Pub:Verifies
UDS	M	F:Obfuscated R:Obfuscated	Device lifetime	F	CDI_n:Derives IDevId:Derives

Table 18: SSP Table 2

SSP Establishment During Device Manufacture or Provisioning

<G1>: Generated within the module on chip.

<IE1>: Written to OTP during device manufacture.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
ROM Integrity		SHA2-256	SW/FW Integrity	fips_status:0	

Table 19: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECC KPDF	P-384	KAT	CAST	fips_status:0	Encrypt	At power-on or reset
Deterministic ECDSA SigGen	P-384, SHA2-384	KAT	CAST	fips_status:0	Generate	At power-on or reset
ECDSA SigVer	P-384, SHA2-384	KAT	CAST	fips_status:0	Verify	Code says driver performs verify
LMS SigVer	SHA2-256	KAT	CAST	fips_status:0	Verify	Code says driver performs verify
FW Load	P-384, SHA2-384	SigVer	Software/Firmware Load	fips_status:0	Encrypt	On FW LOAD command
SHA1	SHA-1	KAT	CAST	fips_status:0	Generate digest	CONFIRM: At power-on or reset

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256	SHA2-256	KAT	CAST	fips_status:0	Generate digest	CONFIRM: At power-on or reset
SHA2-384	SHA2-384	KAT	CAST	fips_status:0	Generate digest	CONFIRM: At power-on or reset
SHA2-384-ACC	SHA2-384	KAT	CAST	fips_status:0	Generate digest	CONFIRM: At power-on or reset

Table 20: Conditional Self-Tests

All cryptographic algorithm self-tests (CASTs) must complete successfully prior to any other use of cryptography by the Module.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ROM Integrity	SHA2-256	SW/FW Integrity	Each use	Power cycle

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECC KPDF	KAT	CAST	Each boot	Reset or power-cycle
Deterministic ECDSA SigGen	KAT	CAST	Each boot	Reset or power-cycle
ECDSA SigVer	KAT	CAST	Each boot	Reset or power-cycle
LMS SigVer	KAT	CAST	Each boot	Reset or power-cycle
FW Load	SigVer	Software/Firmware Load	Each boot	Reset or power-cycle
SHA1	KAT	CAST	Each boot	Reset or power-cycle
SHA2-256	KAT	CAST	Each boot	Reset or power-cycle
SHA2-384	KAT	CAST	Each boot	Reset or power-cycle
SHA2-384-ACC	KAT	CAST	Each boot	Reset or power-cycle

Table 22: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
fips_failure	TBD		Power cycle	fips_status:~0

Table 23: Error States

If one of the CASTs fails, the Module enters the <TBD> state. The error state is persistent, and only <TBD> services are available. All attempts to use the Module's services result in the return of an error code (<specific error code here>). To recover from an error state, the Module must be power-cycled or reset.

10.5 Operator Initiation of Self-Tests

The <TBD> function (inclusive of firmware integrity verification) can be called on demand, fulfilling AS05.11.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Module is based on the open-source Caliptra RTL and Firmware. The Module is provided to vendors who integrate it into their product, typically in a manufacturing environment, and is not provided directly to US or Canadian Federal agencies. Adherence to the instructions in this document maintains security throughout the distribution, build, installation and configuration processes. Tamper is detected via the use of <TBD>. Additional Guidance inclusive of all information required per [ISO19790] Section 7.11.9 is provided by the vendor to the integrator.

11.2 Administrator Guidance

<Text>

11.3 Non-Administrator Guidance

N/A for this module.

11.4 Design and Rules

The inherent properties of the Module are:

1. The Module supports only the Cryptographic Officer role, identified implicitly.
2. The Module does not support a maintenance interface or role.
3. The Module does not support authentication.
4. Power up self-tests do not require any operator action.
5. No additional interface or service is implemented by the Module which would provide access to CSPs.
6. Data output is inhibited during self-tests, zeroization, and error states.
7. The Module does not support manual key entry.
8. The Module does not output plaintext CSPs or intermediate key values.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.

11.5 End of Life [O]

<Text>

12 Mitigation of Other Attacks

12.1 Attack List [O]

The Module implements mitigations for <TBD, e.g., constant-time Implementations>. Constant-time implementations protect cryptographic implementations in the Module against timing analysis since such attacks exploit differences in execution time depending on the cryptographic operation, and constant-time implementations ensure that the variations in execution time cannot be traced back to the key, CSP or secret data.

12.2 Mitigation Effectiveness [O]

<Text>

12.3 Guidance and Constraints [O]

<Text>