EZ Data Shield Sdn Bhd

Taming Sari Crypto Module v1.0

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.6
17 July 2025

EZ Data Shield Sdn. Bhd.
8-23-03 Jalan Medan Pusat Bandar 7A Bangi Sentral
Bandar Baru Bangi
43650 Selangor
Malaysia

Company Registration Number: 202001023360 (1379680-W)
Contact: team@taming-sari.com

Table of Contents

List of Tables

List of Figures

Authors	Title	Date	Version	Description
EZ Data Shield Sdn. Bhd.	Taming Sari Crypto Module v1.0 *FIPS 140-3 Non-Proprietary Security Policy*	27 Dec 2023	v1.0	Initial version.
EZ Data Shield Sdn. Bhd.	Taming Sari Crypto Module v1.0 *FIPS 140-3 Non-Proprietary Security Policy*	18 June 2024	v1.1	Update copyright year, operational environments, cryptographic boundary and CAVP certificate number.
EZ Data Shield Sdn. Bhd.	Taming Sari Crypto Module v1.0 *FIPS 140-3 Non-Proprietary Security Policy*	1 Aug 2024	v1.2	Add and revise several sections related to the Module embodiment, PAA, cryptographic boundary and SSP.
EZ Data Shield Sdn. Bhd.	Taming Sari Crypto Module v1.0 *FIPS 140-3 Non-Proprietary Security Policy*	2 Sep 2024	v1.3	Improve overall technical and editorial content of the document
EZ Data Shield	Taming Sari Crypto Module v1.0 *FIPS 140-3 Non-Proprietary Security Policy*	9 Nov 2024	v1.4	Refine Sections 9.1, 9.4, 10.2, and 11.3, and streamline the document for clarity and consistency.
EZ Data Shield Sdn. Bhd.	Taming Sari Crypto Module v1.0 *FIPS 140-3 Non-Proprietary Security Policy*	22 Nov 2024	v1.5	Refine Sections 2.3, 2.8, 9.3, 9.4, 11 Table 5 and Table 7.
EZ Data Shield Sdn. Bhd.	Taming Sari Crypto Module v1.0 *FIPS 140-3 Non-Proprietary Security Policy*	17 July 2025	v1.6	Refine Table 8, 9, 15.

1 General

1.1 Overview

This document defines the non-proprietary FIPS 140-3 Security Policy for Taming Sari Crypto Module v1.0 cryptographic module (hereafter referred to as “the Module"). The Module is a software cryptographic library in a multi-chip standalone general-purpose computing platform. The security policy outlines the security rules that govern the operations of the Module and explains how the module aligns with the requirements outlined in FIPS 140-3 for a module classified under Security Level 1. The Module meets the overall requirements applicable to this level as shown in **Error! Reference source not found.**.

1.2 Security Levels

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

Table 1: Security Levels

1.3 Additional Information

The following are the definitions for some terms used in this document.

Term	Definition
Critical Security Parameters (CSP)	CSPs contain data whose disclosure or modification can compromise the security of the cryptographic module.
Processor Algorithm Acceleration (PAA)	Acceleration functions supported by processor chips that are deemed a mathematical construct and not the complete cryptographic algorithm (FIPS 140-3 Implementation Guide).
Public Security Parameters (PSPs)	PSPs contain data whose modification can compromise the security of the cryptographic module. Examples include public keys and public key certificates.
Sensitive Security Parameter (SSP)	SSP comprises Critical Security Parameters (CSPs) and Public Security Parameters (PSPs).

Table 2: Terms and Definition

The following are the abbreviations used in this document.

Abbreviations	Term
AES	Advanced Encryption Standard
AES-NI	AES New Instructions
API	Application Programming Interface
CAST	Cryptographic Algorithm Self-Test
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CO	Crypto Officer
CSP	Critical Security Parameter
CTR	Counter Mode
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
FIPS	Federal Information Processing Standards
HMAC	Keyed-Hash Message Authentication Code
KAT	Known-Answer Test
IV	Initialisation Vector
MAC	Message Authentication Code
N/A	Not Applicable
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
PAA	Processor Algorithm Acceleration
PSP	Public Security Parameter
PUB	Publication
RAM	Random Access Memory
SSP	Sensitive Security Parameter

Table 3: Abbreviations

2 Cryptographic Module Specification

2.1 Description

This section provides an overview of the Taming Sari Crypto Module v1.0.

Purpose and Use:

The Module is a software module validated at FIPS 140-3 Security Level 1. It is utilised by the Taming Sari encryption software, the calling application, to provide the necessary cryptographic functionalities required by the software. The Module has been tested on the operational environments listed in **Error! Reference source not found. Error! Reference source not found.**without utilising any processor algorithm acceleration (PAA).

Module Type: Software

Module Embodiment: Multi-Chip Standalone

Module Characteristics:

Cryptographic Boundary:

Figure 1 depicts the operational environment of the Module where the cryptographic boundary is defined within the dotted-line box. The Module includes API functions that can be invoked by calling applications. A pre-operational approved integrity test is performed on all components within the cryptographic boundary.

Tested Operational Environment's Physical Perimeter (TOEPP):

The TOEPP is the general-purpose computer.

Physical Perimeter: General-Purpose Computer

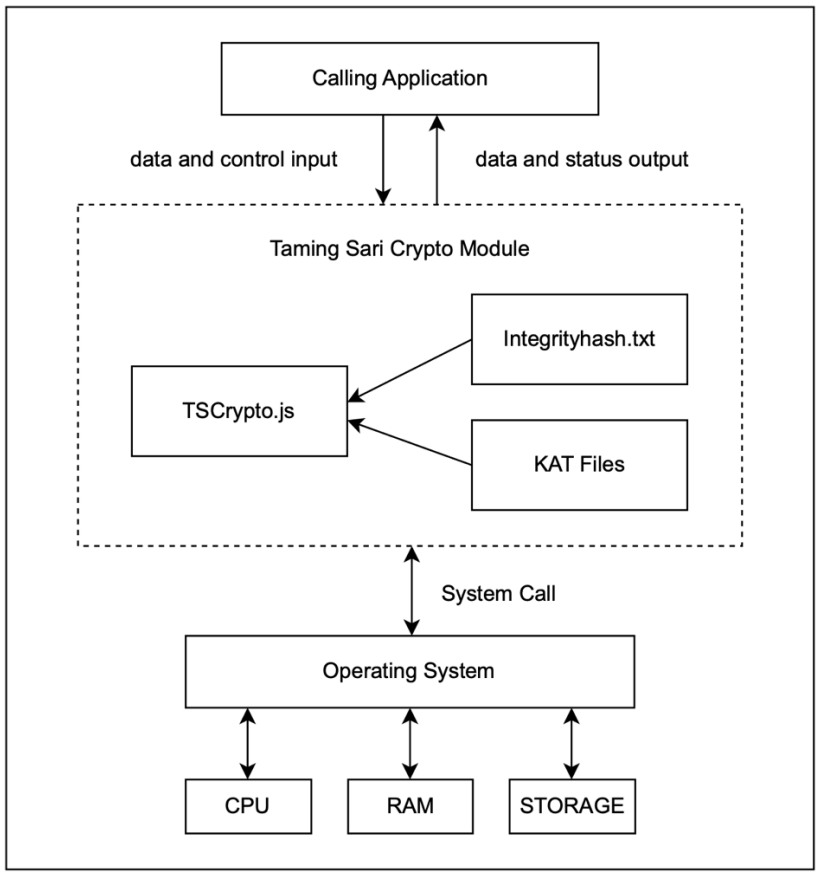

Figure 1: Taming Sari Crypto Module v1.0 cryptographic boundary and physical perimeter

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

Package or File Name	Software/ Firmware Version	Features	Integrity Test
tscrypto-v1-0.zip	v1.0	FIPS 140-3 module	SHA2-512

Table 4: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Windows 11 Pro	Dell XP 8930	Intel Core i7-8700, 3.20GHz	No		v1.0

Table 5: Tested Operational Environments - Software, Firmware, Hybrid

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

N/A for this module as it does not support excluded components.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode of operation	The Module only operates in an Approved mode of operation	Approved	APPROVED

Table 6: Modes List and Description

Mode Change Instructions and Status:

The module only operates in an Approved mode.

Degraded Mode Description:

The Module does not implement a degraded mode.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5346	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A5346	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5346	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
HMAC DRBG	A5346	Prediction Resistance - No Mode - SHA2-512	SP 800-90A Rev. 1
HMAC-SHA2-512	A5346	Key Length - Key Length: 8-2048 Increment 8	FIPS 198-1
SHA2-512	A5346	Message Length - Message Length: 0-1024 Increment 128	FIPS 180-4

Table 7: Approved Algorithms

The module only supports an Approved mode of operation with the algorithms listed in this section. No operational use of an algorithm may be performed until the corresponding CAST has passed.

Vendor-Affirmed Algorithms:

N/A for this module.

The Module does not implement vendor-affirmed algorithms.

Non-Approved, Allowed Algorithms:

N/A for this module.

The Module does not implement non-approved algorithms.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

The Module does not implement non-approved algorithms.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

The Module does not implement non-approved algorithms.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Symmetric encryption and decryption	BC-UnAuth	Unauthenticated Block Ciphers		AES-CBC: (A5346) AES-CTR: (A5346) AES-ECB: (A5346)
Message digest generation	MAC	Hash-Based Message Authentication Codes, MAC tag generation		HMAC-SHA2-512: (A5346)
Secure Hash	SHA	Secure Hash Function		SHA2-512: (A5346)
Deterministic Random Byte Generator	DRBG	Deterministic Random Byte Generator, SHA2-512 with No Prediction Resistance Generator		HMAC DRBG: (A5346)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

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

1. The Module is a software cryptographic library and it is utilized by the calling application. The calling application must ensure that the security functions are used in the correct manner, including generation of the IVs and correct sequencing of the cryptographic operations.
2. The IVs supplied by the calling application for AES in CBC mode must be unpredictable as stipulated in NIST SP800-38A.
3. The calling application is responsible to generate the SSPs used by the Module for cryptographic purposes in accordance with NIST SP800-140D.
4. The Module is installed and configured to Approved mode of operation in accordance with the Module Development and Configuration Management document.
5. Data output is inhibited during self-tests, zeroization, and error states.

2.8 RBG and Entropy

N/A for this module.

N/A for this module.

The only approved deterministic random bit generator (DRBG) provided by the Module is HMAC DRBG using SHA2-512 without prediction resistance. It is used to generate random bytes required by the calling application. Entropy is provided to the Module as a parameter in the DRBG API call. The calling application is responsible for sourcing entropy from an NIST SP800-90B compliant source, which lies outside the Module's boundary. The module enforces a minimum entropy input length of 192 bits. The following caveat applies per FIPS 140-3 IG 9.3.A:

No assurance of the minimum strength of generated SSPs (e.g., keys).

2.9 Key Generation

The Module does not generate SSPs. The calling application is responsible to generate all SSPs which are passed to the API function of the Module.

2.10 Key Establishment

N/A for this module

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
N/A	Data Input	Data inputs are provided in the arguments or parameters passed by the calling application in the API.
N/A	Data Output	Data outputs are returned by the API to the calling application.
N/A	Control Input	Inputs used to control the operation of the Module are provided through API calls.
N/A	Control Output	The Module does not output any commands, signals or control data used to control another module.
N/A	Status Output	Status output is provided via messages. The API Documentation provides description of these return messages.

Table 9: Ports and Interfaces

The Module does not interact with physical ports. The Control Output interface is not applicable, as the Module does not output any commands, signals or control data intended to manage another module.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer (CO)	Role	Crypto Officer (CO)	None

Table 10: Roles

Taming Sari Crypto Module v1.0 only provides support for a single role: the Crypto Officer (CO). There is no support for other roles such as User and Maintenance. FIPS 140-3 Level 1 modules does not require an implementation of the authentication mechanism for the CO. Therefore, the CO does not need to be authenticated to access the Module. The CO is allowed to access all services provided by the Module as listed in **Error! Reference source not found.Error! Reference source not found.**.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
AES encryption / decryption	To perform encryption and decryption operations using the ECB, CBC or CTR mode of operation.	APPROVED	Input for encryption: plaintext, initialisation vector (IV) and key. Input for decryption: ciphertext, IV and key.	Output for encryption: ciphertext. Output for encryption: plaintext.	Symmetric encryption and decryption	Crypto Officer (CO) - AES keys: W,E
Message digest generation	To compute hash digest of a message.	APPROVED	Input: message.	Output: hash value.	Secure Hash	Crypto Officer (CO)
MAC tag generation	To compute the authentication tag of a message.	APPROVED	Input: message and key.	Output: authentication tag.	Message digest generation	Crypto Officer (CO) - HMAC Key: W,E
Random	Generate random	APPROVED	Entropy input	Random Value	Deterministic Random	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	value using the DRBG.		string, Internal State, seed		Byte Generator	(CO) - HMAC DRBG Entropy input: W,E - HMAC DRBG Seed: W,E - HMAC DRBG secret Key value: W,E,Z - HMAC DRBG secret V value: W,E,Z
Zeroisation	To perform zeroisation of SSPs.	APPROVED	Input: handler of security function context.	Output: zeroised SSP	None	Crypto Officer (CO) - AES keys: Z - HMAC Key: Z - HMAC DRBG Entropy input: Z - HMAC DRBG Seed: Z - HMAC DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						secret Key value: Z - HMAC DRBG secret V value: Z
Module Integrity self-test	To perform the pre-operational self-tests.	APPROVED	None	Output: pass/fail status	None	Crypto Officer (CO)
Algorithm KAT	Cryptographic algorithm self-tests	APPROVED	None	Output: pass/fail status	None	Crypto Officer (CO)
Show module status	To display the current operational status of the module.	APPROVED	None	Output: pass/fail status	None	Crypto Officer (CO)
Show module version	To display the module's versioning information.	APPROVED	None	Output: module name and its version number.	None	Crypto Officer (CO)

Table 11: Approved Services

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

N/A for this module.

5 Software/Firmware Security

5.1 Integrity Techniques

Taming Sari Crypto Module v1.0 is a software module and hence, a cryptographic mechanism using an approved integrity technique is applied to all software components within the Module's defined cryptographic boundary as defined in Section 2.1.

A software integrity test is performed on the cryptographic boundary of Taming Sari Crypto Module v1.0 using a hash function. The algorithm used to perform this test is SHA2-512, which is implemented in the Module. The hash computation is compared with a reference hash value that is pre-calculated. As per FIPS 140-3, this referenced hash value is considered as data and itself is not subject to the computation of the integrity technique.

If the integrity test fails, then the Module will enter the Error state where no cryptographic services are provided and the Module is not operational. Upon completion of the integrity test, all temporary values generated during the test is zeroised.

5.2 Initiate on Demand

The integrity test is conducted during the Pre-Operational Self-Tests, automatically initiating upon first use of the Module. It can also be initiated through the self-test service (see **Error! Reference source not found.**) or by reloading the Module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

6.2 Configuration Settings and Restrictions

Specific configuration settings of the Module are covered in the Module Development and Configuration Management document.

7 Physical Security

N/A for this module.

8 Non-Invasive Security

N/A for this module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Storage 1	RAM (Memory)	Dynamic

Table 12: Storage Areas

The Module does not store any SSP persistently beyond the lifetime of an API call.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input 1	EXT: Call stack (API) input parameters	INT	Plaintext	Manual	Electronic	

Table 13: SSP Input-Output Methods

All SSPs are passed in plaintext via API call. The only SSPs passed to the Module is the AES encryption and decryption keys, entropy input string and HMAC key. Furthermore, the Modules does not output any SSPs.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zero 1	Zeroisation of SSPs is performed automatically by API function calls for all temporarily stored SSPs	The API overwrites the temporarily stored SSPs with an empty string	API
Zero 2	When calling application unloads the Module	Temporarily stored SSPs become inaccessible after the application is unloaded, and the memory that was previously allocated is implicitly deallocated.	Occurs when module is unloaded

Table 14: SSP Zeroization Methods

The module supports an implicit zeroisation indicator. The implicit indicator is the successful completion of the service call.
Zeroisation of SSPs is performed automatically by API function calls by overwriting them with the empty string.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES keys	AES encryption/ decryption	128, 192, 256 bits -	Symmetric Key - CSP - CSP			Symmetric encryption

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		128, 192, 256 bits				and decryption
HMAC DRBG Entropy input	Entropy input bit from the external entropy source for DRBG seeding.	256 - 256	Other - CSP - CSP			Deterministic Random Byte Generator
HMAC DRBG Seed	Seed used for DRBG Instantiation.	256 - 256	Other - CSP - CSP			Deterministic Random Byte Generator
HMAC Key	Keyed Hash key	512 - 256	Symmetric Key - CSP - CSP			Message digest generation
HMAC DRBG secret Key value	HMAC DRBG Internal State Secret key value	256 - 256	Other - CSP - CSP			Deterministic Random Byte Generator
HMAC DRBG secret V value	HMAC DRBG Internal State Secret value	256 - 256	Other - CSP - CSP			Deterministic Random Byte Generator

Table 15: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES keys	Input 1	Storage 1:Plaintext	Call lifetime	Zero 1	
HMAC DRBG Entropy input	Input 1	Storage 1:Plaintext	Call lifetime	Zero 1	HMAC DRBG Seed:Constituent
HMAC DRBG Seed	Input 1	Storage 1:Plaintext	Call lifetime	Zero 2	HMAC DRBG secret Key value:Derived From HMAC DRBG Entropy input:Incorporates
HMAC Key	Input 1	Storage 1:Plaintext	Call lifetime	Zero 1	
HMAC DRBG secret Key value	Input 1	Storage 1:Plaintext	Call lifetime	Zero 2	HMAC DRBG Seed:Derived From HMAC DRBG secret V value:Used With
HMAC DRBG secret V value	Input 1	Storage 1:Plaintext	Call lifetime	Zero 2	HMAC DRBG Seed:Derived From HMAC DRBG secret Key value:Used With

Table 16: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
SHA2-512 (A5346)	Module integrity test	known-answer test (KAT)	SW/FW Integrity	SELF-TEST & ERROR	The output of this computation will be compared with a pre-calculated reference hash digest.

Table 17: Pre-Operational Self-Tests

The pre-operational self-tests are performed after the Module has been instantiated and before it enters the operational state. The Module performs a software integrity test of all components within the cryptographic boundary using SHA2-512. Prior to using SHA2-512, a known-answer test (KAT) on the algorithm is performed, which is part of the conditional self-tests (see Section 10.2).

If the KAT on SHA2-512 is successful, only then the Module will perform the actual software integrity test using SHA2-512. The output of this computation will be compared with a pre-calculated reference hash digest. If they match, then the integrity of the Module is assured. Else, the Module is assumed to have been tampered with and will enter the Error state. As per FIPS 140-3 Level 1 specifications, the reference hash digest value is considered data and itself not subject to the integrity technique.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC_Encrypt	128, 192 and 256-bit	known-answer test (KAT)	CAST	SELF-TEST & ERROR	Encrypt	Performed on module load
AES-CBC_Decrypt	128, 192 and 256-bit	known-answer test (KAT)	CAST	SELF-TEST & ERROR	Decrypt	Performed on module load
AES-CTR_Encrypt	128, 192 and 256-bit	known-answer test (KAT)	CAST	SELF-TEST & ERROR	Encrypt	Performed on module load
AES-CTR_Decrypt	128, 192 and 256-bit	known-answer	CAST	SELF-TEST & ERROR	Decrypt	Performed on module load

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
		test (KAT)				
AES-ECB_Encrypt	128, 192 and 256-bit	known-answer test (KAT)	CAST	SELF-TEST & ERROR	Encrypt	Performed on module load
AES-ECB_Decrypt	128, 192 and 256-bit	known-answer test (KAT)	CAST	SELF-TEST & ERROR	Decrypt	Performed on module load
HMAC-SHA2-512 (A5346)	512	known-answer test (KAT)	CAST	SELF-TEST & ERROR	Verify	Performed on module load
SHA2-512 (A5346)	512	known-answer test (KAT)	CAST	SELF-TEST & ERROR	Verify	Performed on module load
HMAC DRBG (A5346)	Instantiate, generate, and reseed as per section 11.3 of SP 800-90A	known-answer test (KAT)	CAST	SELF-TEST & ERROR	Verify	Performed on module load

Table 18: Conditional Self-Tests

The conditional self-tests performed by the Module include KAT for AES in ECB and CBC modes, SHA2-512, HMAC-SHA512 and HMAC-SHA512 DRBG.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-512 (A5346)	known-answer test (KAT)	SW/FW Integrity	On demand by API invocation.	On module load or manual API invocation

Table 19: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC_Encrypt	known-answer test (KAT)	CAST	On demand by API invocation	On module load or manual API invocation
AES-CBC_Decrypt	known-answer test (KAT)	CAST	On demand by API invocation	On module load or manual API invocation

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CTR_Encrypt	known-answer test (KAT)	CAST	On demand by API invocation	On module load or manual API invocation
AES-CTR_Decrypt	known-answer test (KAT)	CAST	On demand by API invocation	On module load or manual API invocation
AES-ECB_Encrypt	known-answer test (KAT)	CAST	On demand by API invocation	On module load or manual API invocation
AES-ECB_Decrypt	known-answer test (KAT)	CAST	On demand by API invocation	On module load or manual API invocation
HMAC-SHA2-512 (A5346)	known-answer test (KAT)	CAST	On demand by API invocation	On module load or manual API invocation
SHA2-512 (A5346)	known-answer test (KAT)	CAST	On demand by API invocation	On module load or manual API invocation
HMAC DRBG (A5346)	known-answer test (KAT)	CAST	On demand by API invocation	On module load or manual API invocation

Table 20: Conditional Periodic Information

The Module permits operators to initiate the pre-operational or conditional self-tests on demand for periodic testing of the module. This can be performed by calling the self-test service via the Module's API. The tests will also be executed whenever the module is reloaded.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Self-Test Failure	Error state for self-test	If one of either integrity test or KAT fails.	The module needs to be restarted or reinitiated. If the error persists even after this process has been per- formed, then contact EZ Data Shield	ERROR

Table 21: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Cryptographic Officer (CO) must utilize the **Taming Sari Guidance Document**, including the **Module Development and Configuration Document**, **Application Programming Interface (API)**, and **Module Design Document**. The **Module Development and Configuration Document** includes a section specific to the Operational Environment (OE) listed in **Error!**

Reference source not found.: Tested Operational Environments. Adherence to the instructions in this document is essential for achieving FIPS 140-3 compliance. Failure to follow these instructions will render the Module noncompliant.

The **Module Development and Configuration Document** outlines procedures for verifying the integrity of the distributed Module. The Module is delivered as a compressed file containing all necessary files for proper execution. Before decompressing this file, users must perform an integrity check by comparing the file's hash value with the reference hash provided by EZ Data Shield. If the hash values match, the Module is safe to use; otherwise, the Module may have been tampered with during transit, and users should immediately contact EZ Data Shield.

Only after a successful integrity check should the compressed file be decompressed. EZ Data Shield assumes no responsibility if users fail to perform this check before decompressing the file. The decompressed file contains the essential components for the Module's operation, and users must not modify any of these files to ensure proper functionality. The **Module Development and Configuration Document** also provides detailed installation instructions for integrating the Module into the calling application.

The Module is embedded within the Taming Sari encryption software and delivered securely to users (e.g., developers of Taming Sari software) through encrypted email attachments or other secure channels. It is not available as a standalone cryptographic library.

11.2 Administrator Guidance

The CO shall use the provided Taming Sari Guidance Document, Module Development and Configuration Management and Module Design Document.

11.3 Non-Administrator Guidance

The Module supports only the CO role and does not accommodate non-administrator roles. As such, guidance for non-administrators is not applicable to this Module.

12 Mitigation of Other Attacks

The Module does not claim mitigation of other attacks.