Ampex Data Systems Corporation

TuffServ® Encryption Module (TSEM)

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.11

May 29, 2024

Prepared for:

Ampex Data Systems Corporation
26460 Corporate Avenue, Suite 200
Hayward, CA 94545
ampex.com
+1 650.367.2011

Prepared by:

KeyPair Consulting Inc.
987 Osos Street
San Luis Obispo, CA 93401
keypair.us
+1 805.316.5024

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document defines the Security Policy for the *TuffServ® Encryption Module* by Ampex, hereafter denoted the "TSEM". The TSEM:

- is a non-modifiable environment.
- does not implement mitigations of attacks outside the scope of the FIPS 140-3 specification.

The TSEM is validated to FIPS 140-3 overall Level 2 requirements with security levels as specified in Section 1.2.

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	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	3
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The hardware TSEM is a multichip embedded embodiment in FIPS 140-3 terminology. The TSEM provides cryptographic key management services for the TuffServ® secure storage device.

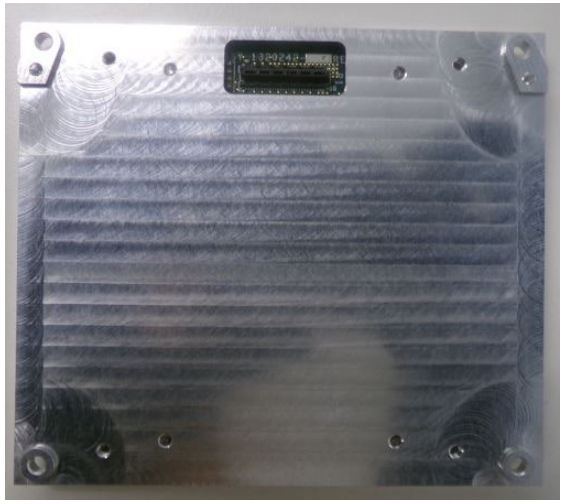
Module Type: Hardware

Module Embodiment: MultiChipEmbed

Cryptographic Boundary:

The Tested Operational Environment's Physical Perimeter (TOEPP) is depicted in Figure 1. The cryptographic boundary is the metal enclosure and the P1 connector on the back of the enclosure. The enclosure opening for the P1 connector does not expose any circuitry except for the P1 connector and associated traces or decoupling capacitors.

Front of Module



Back of Module with P1 Connector

Top of Module (Location of Tamper Seal #1)

Bottom of Module (Location of Tamper Seal #2)

Figure 1: TSEM Physical Perimeter

The TSEM logical functionality (outlined in red) in the context of the larger TuffServ® product is shown in Figure 2. The two SATA controllers (SATA CTL) implement all data plane functionality, including AES XTS data encryption and decryption to and from the storage media. The SoC implements control plane functionality, such as module initialization, configuration, and provisioning. All TSEM firmware is contained within the boundary.

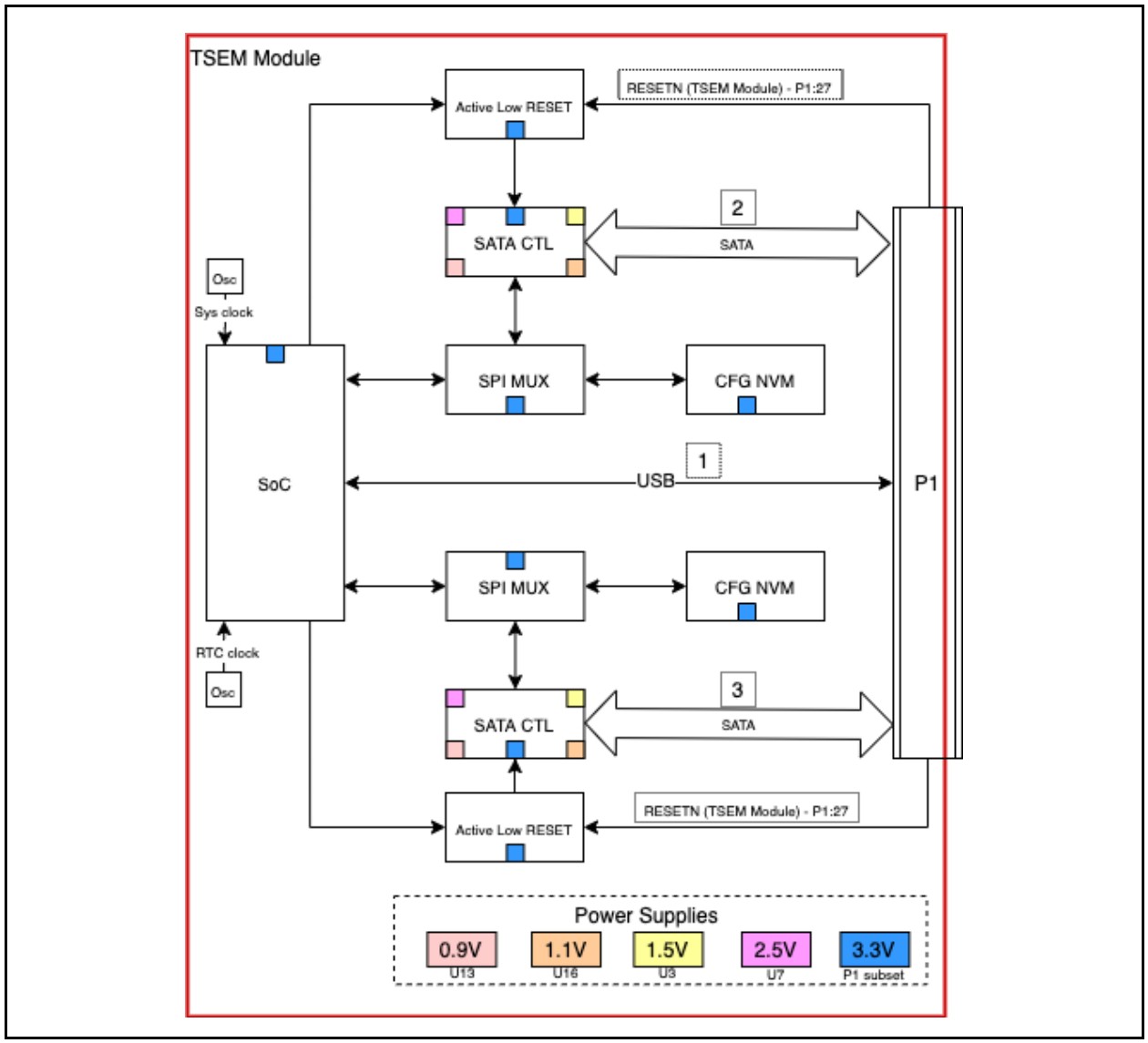


Figure 2: Block Diagram

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
TSEM	1320249-010 Rev A	1.1.16	NXP K81 (ARM Cortex M4)	N/A - only one TSEM model exists.

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

N/A for this Module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	Approved mode of operation	Approved	

Table 3: Modes List and Description

The TSEM supports only an Approved mode of operation, with no configuration necessary to operate and remain in the Approved mode. The TSEM design corresponds to the TSEM security rules specified in Section 11.4.

2.5 Algorithms

Approved Algorithms:

Cipher

Algorithm	CAVP Cert	Properties	Reference
AES-XTS Testing Revision 2.0	A2914	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
AES-ECB	A2921	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-KW	A2921	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38F
AES-ECB	A3009	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A

Table 4: Approved Algorithms - Cipher

Signature

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigVer (FIPS186-4)	A2921	Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-4

Table 5: Approved Algorithms - Signature

Random

Algorithm	CAVP Cert	Properties	Reference
Hash DRBG	A2921	Prediction Resistance - No Mode - SHA2-256	SP 800-90A Rev. 1

Table 6: Approved Algorithms - Random

Message authentication

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-384	A2921	Key Length - Key Length: 256	FIPS 198-1

Table 7: Approved Algorithms - Message authentication

Key derivation

Algorithm	CAVP Cert	Properties	Reference
KDF SP800-108	A2921	KDF Mode - Counter Supported Lengths - Supported Lengths: 256	SP 800-108 Rev. 1

Table 8: Approved Algorithms - Key derivation

Message digest

Algorithm	CAVP Cert	Properties	Reference
SHA2-256	A2921	Message Length - Message Length: 256-2048 Increment 128	FIPS 180-4
SHA2-384	A2921	Message Length - Message Length: 256-2048 Increment 128	FIPS 180-4

Table 9: Approved Algorithms - Message digest

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG Section 4	Key Type:Symmetric	TSEM Cryptographic Library	NIST, SP 800-133 Rev. 2
CKG Section 6.1	Key Type:Symmetric	TSEM Cryptographic Library	NIST, SP 800-133 Rev. 2
CKG Section 6.2	Key Type:Symmetric	TSEM Cryptographic Library	NIST, SP 800-133 Rev. 2

Table 10: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this Module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this Module.

Non-Approved, Not Allowed Algorithms:

N/A for this Module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Cipher	BC-UnAuth	AES-XTS encryption and decryption for data storage		AES-XTS Testing Revision 2.0 AES-ECB
CKG Section 4	CKG	Using the Output of a Random Bit Generator		CKG Section 4
CKG Section 6.1	CKG	Direct Generation of Symmetric Keys		CKG Section 6.1
KTS	KTS-Wrap	SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G	KTS:256 bit keys providing 256 bits of encryption strength	AES-KW AES-ECB
Signature ECDSA	DigSig-SigVer	Signature verification		ECDSA SigVer (FIPS186-4) SHA2-384
Key derivation	CKG KBKDF MAC	Key-based key derivation (KBKDF) for key establishment.		HMAC-SHA2-384 SHA2-384 KDF SP800-108 CKG Section 4 CKG Section 6.2
Random	CKG ENT-P	Generate random value		Hash DRBG SHA2-256

Table 11: Security Function Implementations

2.7 Algorithm Specific Information

XTS-AES:

In accordance with SP 800-38E, the XTS-AES algorithm is to be used for confidentiality on storage devices. The TSEM complies with FIPS 140-3 IG C.I by:

- Generating Key_1 and Key_2 independently according to the rules for component symmetric keys from SP 800-133 Rev. 2 Section 6.3.
- Explicitly checking that Key_1 ≠ Key_2 before using the keys in the XTS-AES algorithm to process data with them.

2.8 RBG and Entropy

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
ENT K81	Physical	K81	1024 bytes	811 bits	N/A

Table 12: Entropy Sources

The entropy source does not have an ESV certificate. In accordance with FIPS 140-3 IG 9.3.A option 1(a), the TSEM generates ENT within the module boundary using a SP 800-90B compliant ENT (P) present on the SoC component.

Per SP 800-90A Rev. 1 Table 2, the SHA2-256 Hash_DRBG requires 256 bits of entropy (equivalent to security strength) within the 440-bit *DRBG_Seed* value. As input to the SP 800-90A Rev. 1 Hash_df, the TSEM collects 1024 bytes of data from the ENT (P) to use as entropy and nonce input. The SP 800-90B compliant assessment supports at least 0.099 bits of entropy per bit of ENT (P) output; as such the DRBG seeding material contains at least 811 bits of entropy, well in excess of the requirement for generating the largest key size of 256 bits.

2.9 Key Generation

The TSEM performs symmetric key generation per FIPS 140-3 IG D.H (direct output of the DRBG):

- Random values are produced in accordance with SP 800-133 Rev. 2 Section 4, in that the DRBG output is provided directly as the random output.
- All usage of DRBG output is of the form B = U⊕V, where V = 0.
- Symmetric keys are generated directly by the DRBG in accordance with SP 800-133 Rev. 2 Section 6.1.

The TSEM also performs derivation of symmetric keys in accordance with SP 800-133 Rev. 2 Section 6.2.

2.10 Key Establishment

Key agreement: N/A for this Module.

Key transport: The Module uses AES-KW with AES-256, which provides 256 bits of strength. This is an Approved key transport method compliant with SP 800-38F and FIPS 140-3 IG D.G.

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
P1: USB1.1 – full speed, 12 MB/s Dedicated Virtual Serial Port over USB.	Data Input Data Output Control Input Status Output	Proprietary control plane commands and responses to and from host (TSEM configuration and control). Does not respond as a general-purpose USB port.
P1: SATA III I/O	Data Input Data Output Control Input Control Output Status Output	Data plane: interaction between host and drive media via controller. SATA commands/responses/status to/from host. Plaintext Data In/Out (from/to host). Ciphertext Data Out/In (to/from media).
P1: RESETN TSEM reset input, active low	Control Input	Low pulse results in TSEM reset.
P1: Power and ground connections	Power	N/A

Table 13: Ports and Interfaces

The P1 connector, shown in Figure 1, is the only physical port of the TSEM. It incorporates all of the specified interfaces.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
PIK Provided	Receipt of PIK by a provisioned TSEM provides role-based authentication of an operator in the User role. The 256-bit PIK is used to derive the 256-bit TIK, which in turn is used to unwrap the TMK. Success of the TMK key unwrap authenticates the caller and unlocks the TSEM, moving it to the Operational state.	KDF SP800-108	1/(2^256) = 8.6E-78	(60*100,000,000)/(2^256) = 5.2E-70

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Signature Verification	Verification of signed command (ECDSA P-384 / SHA-384). All commands that require CO authentication include a corresponding authentication block (signature value) in the command. The value must be verified for the command to be executed.	Signature ECDSA	1/(2^192) = 1.6E-58	(60*100,000,000)/(2^192) = 9.6E-51

Table 14: Authentication Methods

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO	Role	CO	Signature Verification
User	Role	User	PIK Provided

Table 15: Roles

The CO and the User roles are implicitly identified by the service requested.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Initialize	Power-on initialization, including DRBG instantiate and Built-In Test (BIT) with CASTs and FW integrity.	None	None (automatic invocation at power-on / reset).	CPSW (on first command)	Random	Unauthenticated - DRBG_EI: G,E,Z - DRBG_C: G,W - DRBG_V: G,W - DRBG_Seed: G,E,Z
create_keys	Derive TIK from PIK. Use TIK to obtain KEK. Generate DEKs (compliant with SP800-133r2 CKG) and wrap using KEK. Return wrapped DEKs.	TSEM_STATUS_OK or error code	create_keys command packet, PIK, command signature.	CPSW; eDEK	Cipher CKG Section 4 CKG Section 6.1 KTS Signature ECDSA Key derivation	CO - COA Public: E - PIK: W,E,Z - TIK: G,E,Z - TMK: G,E - KEK: G,E,Z - DRBG_C: W,E - DRBG_V: W,E - DEK: G,R,Z
create_random	Obtain a random value.	TSEM_STATUS_OK or error code	create_random command packet .	CPSW; random value	Random CKG Section 4	Unauthenticated - DRBG_EI: G,E,Z - DRBG_C: G,W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG_Seed: G,E,Z
destroy	Halt and reset SATA controllers. Destroy CSPs in local memory and NVM.	TSEM_STATUS_OK or error code	destroy command packet, command signature.	CPSW	Signature ECDSA	CO - COA Public: E,Z - DEK: Z - TMK: Z - DRBG_C: Z - DRBG_EI: Z - DRBG_Seed: Z - DRBG_V: Z - KEK: Z - PIK: Z - TIK: Z
do_bit	Perform built-in test (including FIPS 140 self-tests).	TSEM_STATUS_OK or error code	do_bit command packet, self-test selection.	CPSW; self-test results	None	Unauthenticated
get_bit_results	Obtain status of the most recent built-in tests.	TSEM_STATUS_OK	get_bit_results command packet, self-test selection.	CPSW; self-test results	None	Unauthenticated
nop	Check TSEM responsiveness without performing an operation.	TSEM_STATUS_OK	nop command; no additional input.	CPSW	None	Unauthenticated
provision	Derive TIK from PIK. Wrap TMK using TIK. eTMK refers to the wrapped TMK.	TSEM_STATUS_OK or error code	provision command packet, PIK, TMK, command signature.	CPSW	Signature ECDSA Key derivation	CO - COA Public: E - PIK: W,E,Z - TIK: G,E,Z - TMK: W,Z
put_keys	Derive TIK from PIK. Use TIK to obtain KEK. Use KEK to unwrap DEK. Update SATA controller.	TSEM_STATUS_OK or error code	put_keys command packet, PIK, command signature.	CPSW	Cipher CKG Section 4 CKG Section 6.1 KTS Signature ECDSA Key derivation	CO - COA Public: E - PIK: W,E,Z - TIK: G,E,Z - TMK: G,E - KEK: G,E,Z - DEK: G,R,Z
SATA reset	Reset the SATA controllers.	SATA_OK	SATA reset command.	CPSW.	None	Unauthenticated
status	Return status, name, version.	TSEM_STATUS_OK	This service is not authenticated per FIPS140-3_IG 4.1.A.	CPSW; TSEM name, status, version info	None	Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
read	Read decrypted data from media.	SATA_OK or error code	SATA read command input.	SATA response, data from storage	Cipher	User - DEK: E
write	Write encrypted data to media.	SATA_OK or error code	SATA write command input, data to storage.	SATA response	Cipher	User - DEK: E
Media control	Non-cryptographic SATA commands.	SATA_OK or error code	SATA media control command input.	SATA response	None	Unauthenticated

Table 16: Approved Services

The TSEM supports two status mechanisms: *nop* returns minimal status information, *status* returns additional information. A return code of 0 represents a state without errors. Any other return code is the specific function error of the TSEM.

The phrase “self-test selection” in *do_bit* and *get_bit_results* commands refers to an enumerated target of self-tests, which can specify the firmware integrity test, subsets of CASTs or SATA controller self-tests. “BIT” refers to built-in tests.

eDEK and eTMK refer to the wrapped set of AES XTS (DEK) keys or wrapped TMK, respectively.

CPSW (control plane status word): the Approved mode indicator and success or failure (enumerated) status.

The Indicator column above shows all possible (success or failure) indicator values. The TSEM is a slave device and as such can return status only when it receives a command. If the TSEM fails any CAST or firmware integrity test, it will respond as described in Section 10.4. The return code TSEM_STATUS_OK confirms normal successful completion of the command in the Approved mode, similar to FIPS 140-3 IG 2.4.C example scenario 2, a global indicator for modules having Approved services only.

The relationship of SSPs and security functions is detailed next, using the following notation based on the cited specifications:

SP 800-38F Authenticated encryption: *Ciphertext (wrapped) Key* = KW-AE (*Wrapping Key*, *Plaintext Key*).

SP 800-38F Authenticated decryption: *Plaintext key* = KW-AD (*Wrapping Key*, *Ciphertext (wrapped) Key*).

SP 800-90A Rev. 1 DRBG Generate (Length): generate *Length* random bits.

SP 800-108 Rev. 1 Key Based Key Derivation Function (KBKDF) used to derive symmetric *Key Material* from a *Key Derivation Key*. The TSEM uses the Counter mode with HMAC as PRF.

Key Material = KBKDF (Key Derivation Key, Label, Context, Length)

- *Label*: binary string that identifies the purpose for the derived keying material.
- *Context*: a binary string used to bind the derived value to an entity or process.
- *Length* of material to be derived in bits.

The notation e*Keyname* refers to *Keyname* in encrypted (ciphertext) form. It is not a different CSP.

create_keys

[1] Verify command (with COA Public).

[2] TIK = KBKDF (PIK): Derive TIK from PIK.
[3] TMK = KW-AD (TIK, eTMK): Use TIK to obtain KEK.
[4] KEK = KBKDF (TMK). Generate DEKs and wrap using KEK. Return wrapped DEKs. (eDEK refers to the wrapped DEK.)
[5] DEK = DRBG Generate.
[6] Verify AES XTS non-equal.
[7] eDEK = KW-AE(KEK, DEK).

create_random

Performs a DRBG generate. DRBG_EI is used to seed as required. Random generation updates the DRBG_State.

destroy

[1] Verify command (with COA Public).
[2] Halt / reset SATA controllers.
[3] Overwrite RAM CSPs.
[4] Erase NVM CSPs.

do_bit, ***get_bit_results***, ***nop***, ***status*** and ***Media control*** do not utilize approved security functions or access SSPs. The term "bit" refers to built-in self-test functionality.

The ***nop*** command provides a mechanism to check simple status; the ***status*** command provides extended status information, including name and version correlatable to the CMVP listing (as required by ISO/IEC 19790:2012 AS04.13). The ***status*** command response (intended for use by the host device driver) is a binary structure encoded in Base64 for transfer. When translated to ASCII, the response includes the module name ("TSEM") as well as version information for the SoC and the SATA controllers.

provision

[1] Verify command (COA Public).
[2] TIK = KBKDF (PIK): Derive TIK from PIK.
[3] eTMK = KW-AE (TIK, TMK): Wrap TMK using TIK. (eTMK refers to the wrapped TMK.)

put_keys

Update SATA controller.
[1] Verify command (COA Public).
[2] TIK = KBKDF (PIK): Derive TIK from PIK.
[3] TMK = KW-AD (TIK, eTMK): Use TIK to obtain KEK.
[4] KEK = KBKDF (TMK): Derive KEK from TMK.
[5] DEK = KW-AD (KEK, eDEK): Use KEK to unwrap DEK.
[6] Verify AES XTS key constituents are non-equal.
[7] Update SATA controller DEK.

SATA reset

Resets the SATA engine hardware, zeroizing the DEK SSPs in both channels. The DEK keys are erased from SATA controller registers but remain intact in the TSEM RAM.

read

Decrypts the data using AES-XTS; supports 2 channels of decryption with separate keys.

Write

Encrypts the data using AES-XTS; supports 2 channels of encryption with separate keys.

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

The TSEM uses ECDSA P-384 SHA2-384 signature verification performed over all module firmware as the integrity technique.

5.2 Initiate on Demand

The operator can initiate the integrity test on demand by power cycling the module or by issuing the *do_bit* command.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Enclosure tamper seals (qty. 2)	Seals should be inspected during maintenance operations and when circumstances dictate (e.g., if tampering is suspected).	The tamper seals are within recessed seal guides. Inspect tamper seals for evidence of lifted edges or excessive wear.

Table 17: Mechanisms and Actions Required

The hardware TSEM is a multichip embedded embodiment packaged in a metal enclosure. The metal enclosure is protected by two (2) tamper seals placed within the seal guides (milled sections on the enclosure), as shown in **Error! Reference source not found.**. The metal enclosure is opaque in the visible spectrum.

Ampex maintains control over the tamper seals, which may only be applied or replaced in the factory setting.

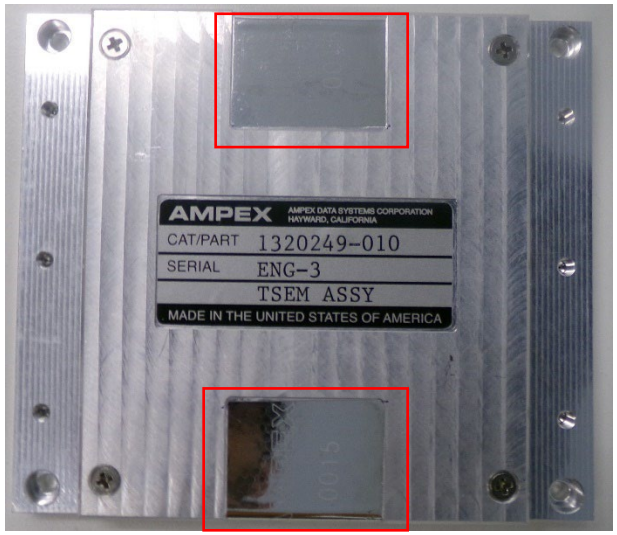


Figure 3: Location of Tamper Seals (Front)

Figure 4: Location of Tamper Seal #1 (Top Edge)

Figure 5: Location of Tamper Seal #2 (Bottom Edge)

8 Non-Invasive Security

N/A for this Module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
SoC FW NVM	Firmware image stored in SoC Non-volatile memory (flash)	Static
SoC RAM	SoC RAM	Dynamic
SATA CTL register	SATA CTL register	Dynamic
SoC NVM	SoC CFG Non-volatile memory (flash)	Static

Table 18: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Ampex facility	Entered in Ampex maintenance facility.	SoC FW NVM	Plaintext	N/A	N/A	
Encrypted input parameter	External source	SATA CTL register	Encrypted	Automated	Electronic	KTS
Encrypted output parameter	SATA CTL register	External source	Encrypted	Automated	Electronic	KTS
Plaintext input parameter	External source	SoC RAM	Plaintext	Automated	Electronic	

Table 19: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
After use	Overwritten by zeros after use	Overwritten with zeros	Module code enforces zeroization after use
Power Cycle	Overwritten by zeros upon loss of power	Overwritten with zeros	Operator can remove power from the module
Destroy	Overwritten by zeros by Destroy service	Overwritten with zeros	Operator calls the destroy service

Table 20: SSP Zeroization Methods

TSEM code destroys all plaintext CSPs prior to return from any control plane command.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
COA Public	Verification of CO operator commands.	Size: 384 - Strength: 192	ECDSA P-384 - PSP			Signature ECDSA

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DEK	AES XTS data encryption keys (DEKC1, DEKC2, DEKD1, DEKD2).	Size: 256 - Strength: 256	Symmetric - CSP	CKG Section 4 CKG Section 6.1		Cipher
DRBG_C	DRBG state value C.	Size: 440 - Strength: 256	Hash_DRBG_C - CSP	Hash DRBG		Hash DRBG
DRBG_EI	DRBG Entropy Input (inclusive of nonce).	Size: 1024 - Strength: 256	Entropy input - CSP			Hash DRBG
DRBG_Seed	DRBG Seed (required per CMVP SSP conventions).	Size: 440 - Strength: 256	DRBG_Seed - CSP	Hash DRBG		Hash DRBG
DRBG_V	DRBG state value V.	Size: 440 - Strength: 256	Hash_DRBG_V - CSP	Hash DRBG		Hash DRBG
KEK	AES-256 key used to wrap DEK keys.	Size: 256 - Strength: 256	Symmetric - CSP	Key derivation		KTS
PIK	Platform Identity Key, used to derive TIK which unwraps TMK; success authenticates host to TSEM.	Size: 256 - Strength: 256	Symmetric - CSP			Key derivation
TIK	TSEM Identity Key: used to wrap the TMK.	Size: 256 - Strength: 256	Symmetric - CSP	Key derivation		KTS
TMK	TSEM Master Key: AES-256 key used to derive KEK.	Size: 256 - Strength: 256	Symmetric - CSP			Key derivation

Table 21: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
COA Public	Ampex facility	SoC NVM:Plaintext	Call lifetime	Destroy	
DEK	Encrypted input parameter Encrypted output parameter	SoC RAM:Plaintext SATA CTL register:Plaintext	Call lifetime	After use Power Cycle Destroy	KEK:Wrapped By
DRBG_C		SoC RAM:Plaintext	Module uptime	After use Power Cycle Destroy	DRBG_V:Used With DRBG_Seed:Derived From
DRBG_EI		SoC RAM:Plaintext	Module uptime	After use Power Cycle Destroy	DRBG_Seed:Incorporated Into
DRBG_Seed		SoC RAM:Plaintext	Module uptime	After use Power Cycle Destroy	DRBG_EI:Constituent DRBG_C:Derives DRBG_V:Derives

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG_V		SoC RAM:Plaintext	Module uptime	After use Power Cycle Destroy	DRBG_C:Used With DRBG_Seed:Generated From
KEK		SoC RAM:Plaintext	Call lifetime	After use Power Cycle Destroy	TMK:Derived From DEK:Wraps
PIK	Plaintext input parameter	SoC RAM:Plaintext	Call lifetime	After use Power Cycle Destroy	TIK:Derives
TIK		SoC RAM:Plaintext	Call lifetime	After use Power Cycle Destroy	PIK:Derived From TMK:Wrapped By
TMK	Plaintext input parameter	SoC NVM:Encrypted	Call lifetime	Destroy	TIK:Wraps

Table 22: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
FW Integrity	ECDSA P-384 #A2921	Signature verification performed over all TSEM firmware at power-up.	SW/FW Integrity	TSEM_STATUS_OK	Verify

Table 23: Pre-Operational Self-Tests

The corresponding ECDSA signature verification CAST is performed prior to the integrity test.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XTS Testing Revision 2.0	256-bit	KAT	CAST	TSEM_STATUS_OK	Encrypt	Performed on module load.
AES-XTS Testing Revision 2.0	256-bit	KAT	CAST	TSEM_STATUS_OK	Decrypt	Performed on module load.
AES-KW	256-bit	KAT	CAST	TSEM_STATUS_OK	Forward cipher	Performed on module load.
AES-KW	256-bit	KAT	CAST	TSEM_STATUS_OK	Inverse cipher	Performed on module load.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-4)	P-384 SHA2-384	KAT	CAST	TSEM_STATUS_OK	Signature verification	Performed on module load prior to firmware integrity test.
Hash DRBG	SHA2-256	KAT	CAST	TSEM_STATUS_OK	Instantiate, generate, reseed	Performed on module load.
KDF SP800-108	HMAC-SHA2-384	KAT	CAST	TSEM_STATUS_OK	SP800-108r1 Section 4.1 KAT for a Counter Mode KDF	Performed on module load.
SHA2-384 (A2921)	SHA2-384	KAT	CAST	TSEM_STATUS_OK	Hash	Performed on module load.
ENT (P) Self-tests	90B Self-tests	CAST	CAST	TSEM_STATUS_OK	90B Health Tests	Performed on module load, power cycle or do_bit service invocation.

Table 24: Conditional Self-Tests

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

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
FW Integrity	Signature verification performed over all TSEM firmware at power-up.	SW/FW Integrity	On demand	Power cycle or do_bit

Table 25: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XTS Testing Revision 2.0	KAT	CAST	On demand	Power cycle or do_bit
AES-XTS Testing Revision 2.0	KAT	CAST	On demand	Power cycle or do_bit
AES-KW	KAT	CAST	On demand	Power cycle or do_bit
AES-KW	KAT	CAST	On demand	Power cycle or do_bit
ECDSA SigVer (FIPS186-4)	KAT	CAST	On demand	Power cycle or do_bit
Hash DRBG	KAT	CAST	On demand	Power cycle or do_bit
KDF SP800-108	KAT	CAST	On demand	Power cycle or do_bit
SHA2-384 (A2921)	KAT	CAST	On demand	Power cycle or do_bit
ENT (P) Self-tests	CAST	CAST	Each use	Continuously running

Table 26: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
ERROR state	Self-test failure error state	If one of the KATs fails or integrity test fails	Power-cycle	Non-zero return status

Table 27: Error States

If one of the CASTs fails, the TSEM enters the ERROR state. The error state is persistent, and only Status services are available. All attempts to use the TSEM's services result in the return of a non-zero error code in the range -40 (TSEM_ERROR_CYBER) to -47 (TSEM_ERROR_CYBER_LYCAN2).

10.5 Operator Initiation of Self-Tests

The TSEM automatically invokes all self-tests on each power-on or reset. The conditional self-tests may also be invoked on demand by the *Self-Test* service *do_bit* command; detailed results are available using the *Self-Test* service *get_BITResults* command.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The TSEM is a subsystem of the TuffServ® product and is not intended for use in other settings. The TSEM User and CO Guide documents all procedures for the following:

- Secure installation, initialization, configuration, and provisioning of the TSEM.
- Secure distribution and delivery of the TSEM.

The module only operates in the Approved mode of operation. There are no maintenance requirements for the TSEM.

11.2 Administrator Guidance

The TSEM User and CO Guide is inclusive of all information required per ISO/IEC 19790:2012 Section 7.11.9.

11.3 Non-Administrator Guidance

The TSEM User and CO Guide is inclusive of all information required per ISO/IEC 19790:2012 Section 7.11.9.

11.4 Design and Rules

The TSEM enforces the following security rules:

1. All services implemented by the module are described in the tables below. The module has no other mechanism which permits access to CSPs.
2. Data output is inhibited during key generation, self-tests, zeroization, and the error state.
3. Control output is inhibited whenever the module is in the error state and during self-tests.
4. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
5. The module does not support manual key entry.
6. The module does not support firmware loading.
7. The module does not output plaintext CSPs or intermediate key values.

8. The module does not allow CSPs entered in the module in encrypted form to be displayed in plaintext.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. The module can use only algorithms that have passed self-tests.
11. The module prohibits changing to the Crypto Officer state from any other role other than the Crypto Officer.
12. The module does not support multiple concurrent operators, a maintenance role or a bypass capability.

11.5 End of Life

The TSEM User and CO Guide documents all procedures for decommissioning and sanitization of the TSEM.

12 Mitigation of Other Attacks

N/A for this Module.