中盛信安
chasesunchn

ChaseSun CS100
FIPS 140-2 Non-Proprietary Security Policy

Document Revision: V1.0
H.W. Version: V1.0.0
F.W. Version: V1.0.0

Revision History

Author(s)	Version	Updates
SunPeng	1.0	12/12/2014

Introduction

The ChaseSun CS100 Cryptographic Module (H.W. Version: 1.0.0 F.W. Version:1.0.0) is a multi-chip embedded cryptographic module designed to decrypt and decode audio/video data for a digital cinema projector.

Cryptographic Boundary

The cryptographic boundary is defined by the area that the hard and opaque metal enclosure covers, which is outlined in yellow in the images below.

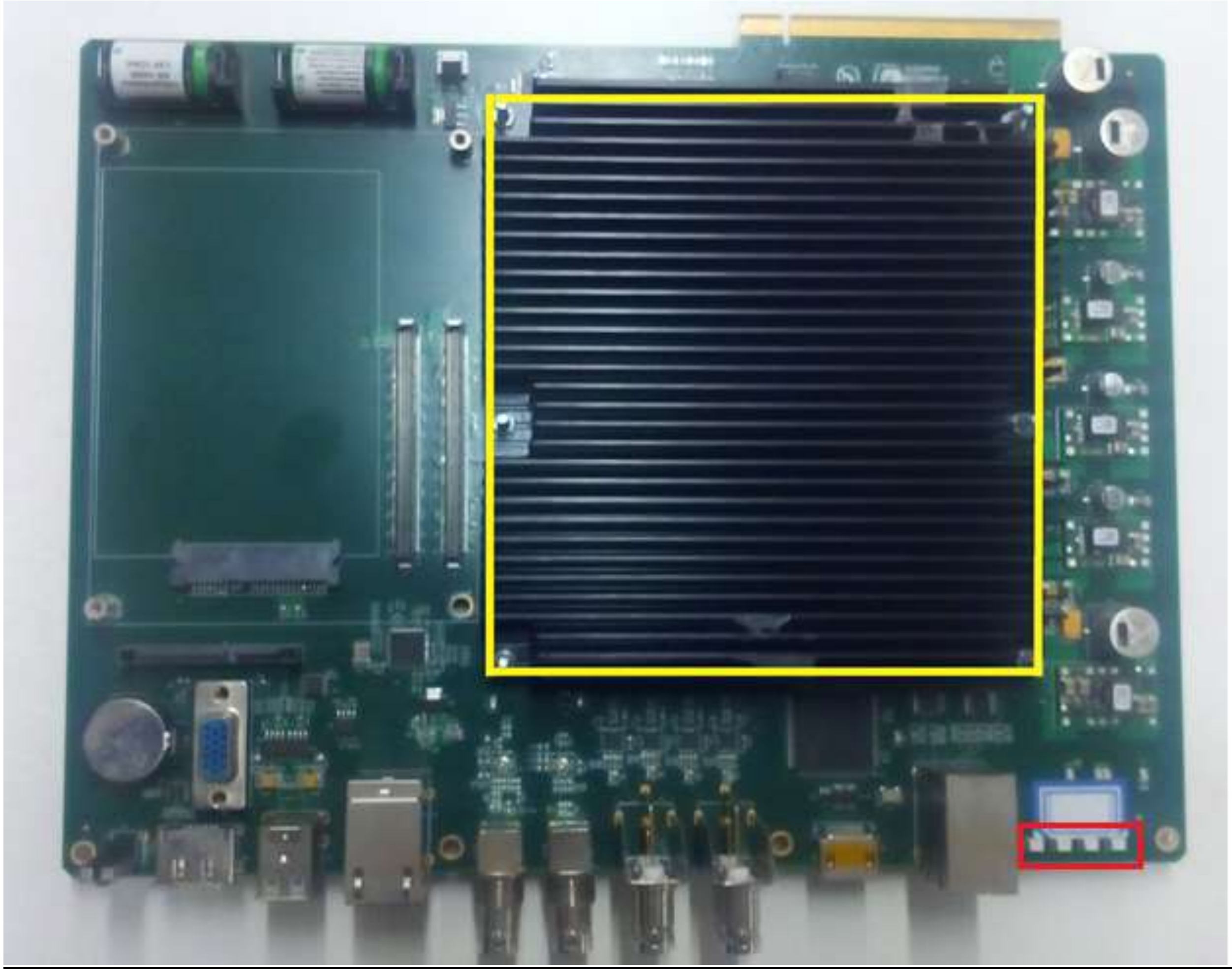

Exhibit 1 –Top view of the cryptographic boundary (Note: location of LEDs that provide status is shown in red)

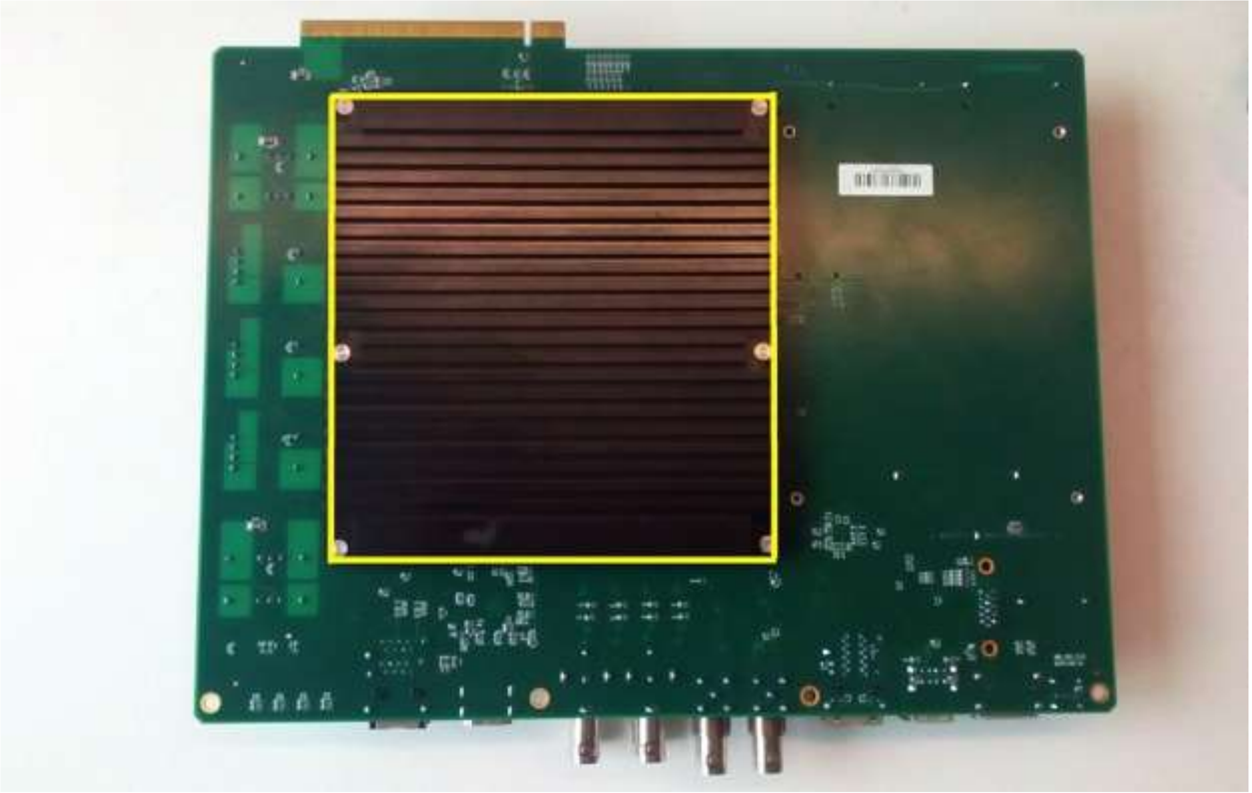

Exhibit 2 –Bottom view of the cryptographic boundary

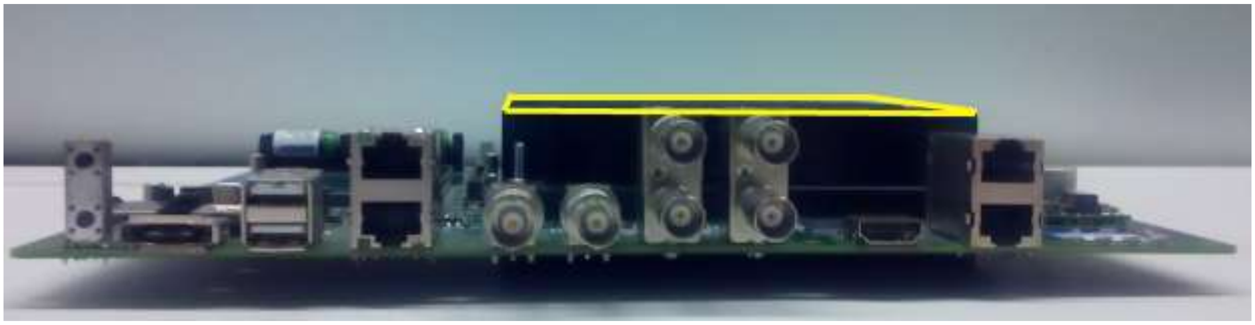

Exhibit 3 –Front view of the cryptographic boundary

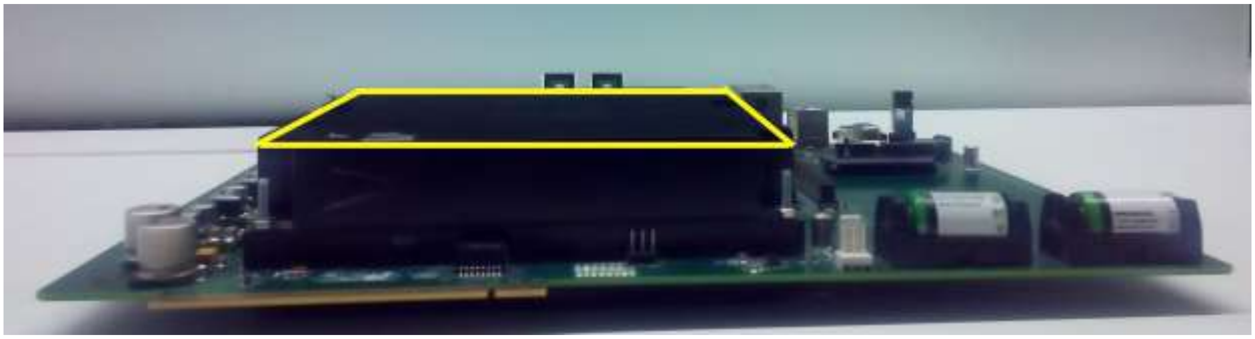

Exhibit 4 –Back view of the cryptographic boundary

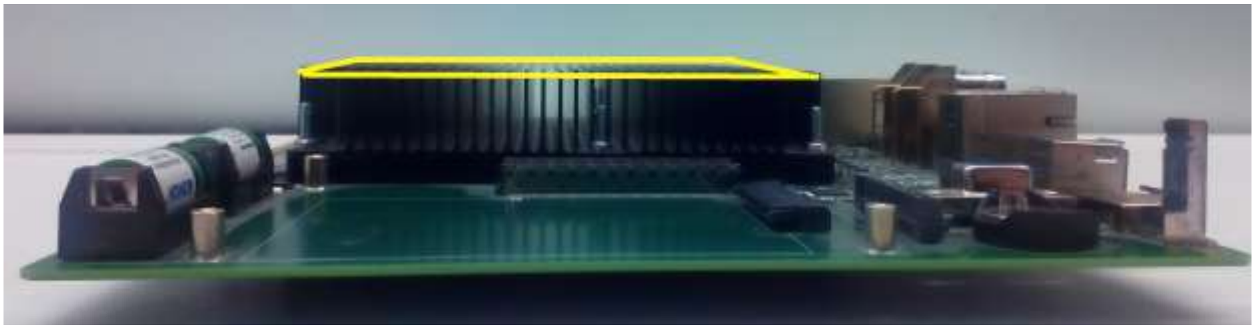

Exhibit 5 –Left view of the cryptographic boundary

Exhibit 6 –Right view of the cryptographic boundary

Security Level

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2.

Security Requirements Section	Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

Exhibit 7- Module Security Level Specification

Physical Ports and Logical Interfaces

The module is a multi-chip embedded module with ports and interfaces as shown below.

Physical Port	Logical Interface
eSATA USB (Qty. 2) Ethernet (Qty. 2) HDMI In	Data Input
Reset Button (Qty. 2) Ethernet (Qty. 2)	Control Input
LVDS video output RJ45 AES Audio Output (Qty. 2)	Data Output
Status LEDs (Qty. 4)	Status Output
Button Battery (Qty. 2)	Power Input

Exhibit 8–Specification of Cryptographic Module Physical Ports and Logical Interfaces

Approved Security Functions

The module only provides a FIPS Approved mode of operation. The module will enter FIPS Approved mode following successful power up self-tests, and will signal this via a green LED in the following manner:
LED #1: Solid Green
LED #2: Off
LED #3: Off
LED #4: Off

The following are Approved Security Functions that the module contains:

1. AES (Certs. #2977 and #2978)
2. RSA (Cert. #1563)
3. SHS (Certs. #2501 and #2502)
4. RNG (Cert. #1302)
5. FIPS 186-2 RNG (Cert. #1336)
6. HMAC (Certs. #1886 and #1887)
7. CVL (Cert. #359)

Non-Approved Security Functions

The cryptographic module supports the following non-FIPS Approved Functions which are allowed for use in FIPS mode.

1. RSA Decrypt: (Used for key unwrapping only, key establishment methodology provides 112 bits of strength)
2. MD5 for use within TLS KDF v1.0/1.1 only
3. NDRNG for the seeding of the ANSI X9.31 RNGs

NOTICE: As per FIPS 140-2 Implementation Guidance D.11, the following notice is included herein: The TLS protocol has not been reviewed or tested by the CAVP and CMVP.

Security rules

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

1. The cryptographic module provides two distinct operator roles: User role and the Cryptographic Officer role.
2. The cryptographic module provides identity-based authentication.
3. The cryptographic module clears previous authentications on power cycle.
4. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
5. The cryptographic module performs the following tests:

   A. Power up Self-Tests

      1. Cryptographic algorithm tests

         a. AES 128-bit Encrypt/Decrypt KATs (CBC mode)
         b. RSA 2048 Sign KAT
         c. RSA 2048 Verify KAT
         d. RSA 2048-bit Decrypt KAT
         e. HMAC-SHA-1 KAT
         f. SHA-1 KAT (Tested as a part of HMAC)
         g. SHA-256 KAT
         h. ANSI X9.31DRNG KAT
         i. FIPS 186-2 RNG KAT
         j. TLS KDF KAT
         k. Firmware Integrity Test – CRC-32
         l. FPGA AES Decrypt KAT
         m. FPGA SHA-1 KAT
         n. FPGA HMAC-SHA-1 KAT

   B. Critical Functions Tests – N/A

   C. Conditional Self-Tests

      a. Continuous Random Number Generator (RNG) test – performed on NDRNG
      b. Continuous Random Number Generator (RNG) test – performed on DRNG
      c. Firmware Update Test – HMAC-SHA-1 (128 bit key) verification
      d. Manual Key Entry Test: N/A
      e. Bypass Test: N/A

6. The operator is capable of commanding the module to perform the power-up self-test by cycling power or resetting the module.
7. Power-up self tests do not require any operator action.

8. Data output is inhibited during key generation, self-tests, zeroization, and error states.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. The module ensures that the seed and seed key inputs to the Approved DRNG are not equal by performing a comparison.
11. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
12. The module does not support concurrent operators.
13. The module does not support a maintenance interface or role.
14. The module does not support manual key entry.
15. The module does not enter or output plaintext CSPs.
16. The module does not output intermediate key values.
17. In the event of a self-test failure, the module provides the following status via LEDs:

    LED #1: Red
    LED #2: Off
    LED #3: Off
    LED #4: Off

Identification and Authentication Policy

The cryptographic module shall support two distinct operator roles: User and Cryptographic-Officer. The Cryptographic-Officer is assumed by ChaseSun and the User is assumed by the SMS (Screen Management System). The cryptographic module shall enforce the separation of roles using identity-based operator authentication by means of RSA 2048 with SHA-256 digital signature verifications.

Role	Type of Authentication	Authentication Data
Cryptographic Officer	Identity-based operator authentication	Digital Signature Verification (RSA 2048 with SHA-256)
User	Identity-based operator authentication	Digital Signature Verification (RSA 2048 with SHA-256)

Exhibit 9- Roles and Required Identification and Authentication
(FIPS 140-2 Table C1)

Define the strength of each implemented authentication mechanism by discussing the probabilities associated with random attempts, and multiple consecutive attempts within a one-minute period to subvert the implemented authentication mechanisms.

Authentication Mechanism	Strength of Mechanism
RSA 2048-bit Digital Signature Verification	The probability that a random attempt will succeed, or a false acceptance will occur, is $1/2^{112}$, which is less than 1/1,000,000. The module can perform RSA signature verification in approximately 172ms, which computes to approximately 350 verifications per minute. Therefore, the probability that a brute force attack being successful within a 1-minute period is 350/(2^112), which is less than 1/100,000.

Exhibit 10- Strengths of Authentication Mechanisms
(FIPS 140-2 Table C2)

Access Control Policy

The following is a list of CSPs and Public Keys that are available to each of the authorized roles via the corresponding services.

Role	Service	Cryptographic Keys, CSPs, and Public Keys	Type(s) of Access
Cryptographic Officer	FW Update: Updates the firmware of the module.	CO Public Key	Read
		CO Root CA Public Key	Read
		CO Sec-Level CA Public Keys	Read
		FW Upgrade Key	Read
		Log Private Key	Read
		Log Public Key	Read
		SM System Public Key	Read
		System Root CA Public Key	Read
		System Sec-Level CA Public Key	Read
		SMS Root CA Public Key	Read
		SMS Sec-Level CA Public Key	Read
		TLS Encryption Key	Generate
		TLS Integrity Key	Generate
		TLS KDF State	Generate
		TLS Pre-Master Secret	Generate

		TLS Master Secret	Generate
	Zeroize: Actively destroys all CSPs contained within the module.	CO Public Key	Zeroize
		CO Root CA Public Key	
		CO Sec-Level CA Public Key	
		Log Private Key	
		Log Public Key	
		SM System Public Key	
		System Root CA Public Key	
		System Sec-Level CA Public Key	
		SMS Root CA Public Key SMS Sec-Level CA Public Key	
		All CSPs	
		TLS Encryption Key	
		TLS Integrity Key	
		TLS KDF State	
		TLS Pre-Master Secret	
		TLS Master Secret	
User	Playback: Includes normal playback functions such as play reel and play control.	SM Private Key	Read
		Log Private Key	Read
		Log Public Key	Read
		SM System Public Key	Read
		System Root CA Public Key	Read
		System Sec-Level CA Public Key	Read
		RNG Seed	Read
		RNG Seed Key	Read
		Content Decryption Key	Read
		Content Integrity Key	Read/Write
		User Public Key	Read
		User Root CA Public Key	Read
		User Sec-Level CA Public Key	Read
		SMS Root CA Public Key	Read
		SMS Sec-Level CA Public Key	Read

		TLS Encryption Key	Generate
		TLS Integrity Key	Generate
		TLS KDF State	Generate
		TLS Pre-Master Secret	Generate
		TLS Master Secret	Generate
		FIPS 186-2 RNG State	Generate
	Configuration: Sets the configuration of MB card.	Log Private Key	Read
		Log Public Key	Read
		SM System Public Key	Read
		System Root CA Public Key	Read
		System Sec-Level CA Public Key	Read
		User Public Key	Read
		User Root CA Public Key	Read
		User Sec-Level CA Public Key	Read
		SMS Root CA Public Key	Read
		SMS Sec-Level CA Public Key	Read
		TLS Encryption Key	Generate
		TLS Integrity Key	Generate
		TLS KDF State	Generate
		TLS Pre-Master Secret	Generate
		TLS Master Secret	Generate
	Export Log: Exports log files from the Security Manager (SM).	Log Private Key	Read
		Log Public Key	Read
		SM System Public Key	Read
		System Root CA Public Key	Read
		System Sec-Level CA Public Key	Read
		User Public Key	Read
		User Root CA Public Key	Read
		User Sec-Level CA Public Key	Read
		SMS Root CA Public Key	Read
		SMS Sec-Level CA Public Key	Read
		TLS Encryption Key	Generate
		TLS Integrity Key	Generate

		TLS KDF State	Generate
		TLS Pre-Master Secret	Generate
		TLS Master Secret	Generate
	GetCertificate: Gets the certificate of the device.	Log Private Key	Read
		Log Public Key	Read
		SM System Public Key	Read
		System Root CA Public Key	Read
		System Sec-Level CA Public Key	Read
		User Public Key	Read
		User Root CA Public Key	Read
		User Sec-Level CA Public Key	Read
		SMS Root CA Public Key	Read
		SMS Sec-Level CA Public Key	Read
		TLS Encryption Key	Generate
		TLS Integrity Key	Generate
		TLS KDF State	Generate
		TLS Pre-Master Secret	Generate
		TLS Master Secret	Generate
	GetVersion: Gets the version of the Media Block.	Log Private Key	Read
		Log Public Key	Read
		SM System Public Key	Read
		System Root CA Public Key	Read
		System Sec-Level CA Public Key	Read
		User Public Key	Read
		User Root CA Public Key	Read
		User Sec-Level CA Public Key	Read
		SMS Root CA Public Key	Read
		SMS Sec-Level CA Public Key	Read
		TLS Encryption Key	Generate
		TLS Integrity Key	Generate
		TLS KDF State	Generate
		TLS Pre-Master Secret	Generate
		TLS Master Secret	Generate
	GetTime: Gets the time of the SM system.	Log Private Key	Read
		Log Public Key	Read
		SM System Public Key	Read
		System Root CA Public Key	Read

		System Sec-Level CA Public Key	Read
		User Public Key	Read
		User Root CA Public Key	Read
		User Sec-Level CA Public Key	Read
		SMS Root CA Public Key	Read
		SMS Sec-Level CA Public Key	Read
		TLS Encryption Key	Generate
		TLS Integrity Key	Generate
		TLS KDF State	Generate
		TLS Pre-Master Secret	Generate
		TLS Master Secret	Generate

Exhibit 11– Services Authorized for Roles, Access Rights within Services
(FIPS 140-2 Table C3, Table C4)

Unauthenticated Services

The following is a list of services that do not require an authorized role. These services do not disclose, modify, or substitute CSPs, use an Approved security function, or otherwise affect the security of the cryptographic module.

Service	Description
Self-tests	This service executes the suite of self-tests required by FIPS 140-2 and is invoked by power cycling or resetting the device.
Get Status	This service provides module status via LEDs.

Exhibit 12–Unauthenticated Services

Physical Security Policy

Exhibit 13 below explains the physical security mechanisms that are implemented by the module and the actions required by the operator to ensure that physical security is maintained.

Physical Security Mechanisms	Recommended Frequency of	Inspection/Test Guidance Details

Hard Opaque Enclosure	Startup module or reboot module	Inspect for scratches or deformation of the metal enclosure. If such evidence is found, the user should not use the module.
Tamper Evident Seals	Startup module or reboot module	Inspect for destruction of the seals. If such evidence is found, the user should not use the module.
Zeroization Switches	Startup module or reboot module	If the module was zeroized, the user should return it to ChaseSun.

Exhibit 13- Inspection/Testing of Physical Security Mechanisms
(FIPS 140-2 Table C5)

The module requires (Qty. 2) tamper labels, and placement of these labels can be seen in the Exhibit 14 below.

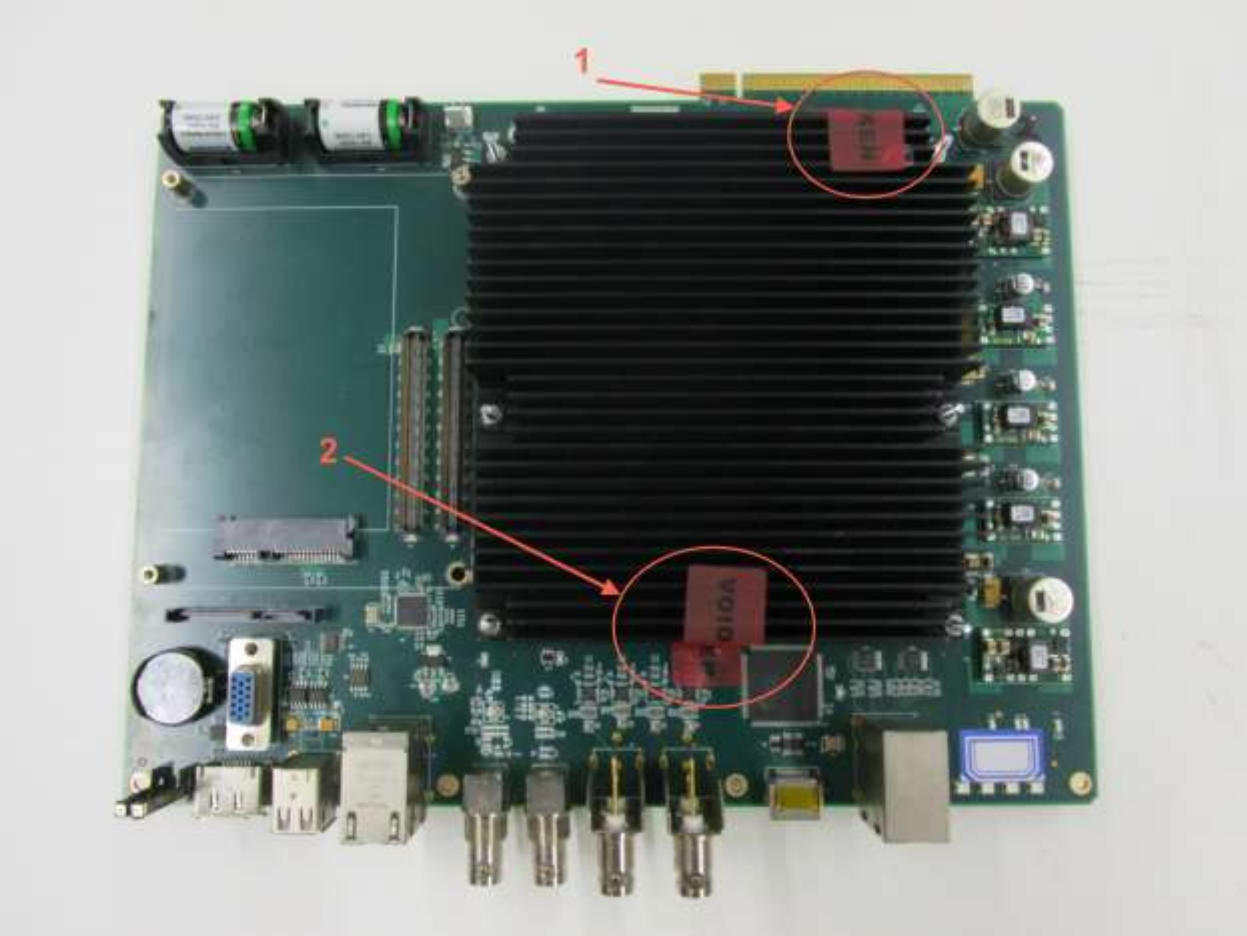

Exhibit 14- Tamper label placement on the ChaseSun CS100 module

Mitigation of Other Attacks Policy

The module has not been designed to mitigate against any attacks that are outside of the scope of FIPS 140-2.

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

Exhibit 15- Mitigation of Other Attacks
(FIPS 140-2 Table C6)