NON-PROPRIETARY SECURITY POLICY FOR BLACK LANTERN® CRYPTOGRAPHIC MODULE

1700 DIAGONAL ROAD
SUITE 320
ALEXANDRIA, VA 22314

DOCUMENT NUMBER: BL400-A1-SP
REVISION: -
DATE: 30 August 2022

TABLE OF CONTENTS

1 Introduction 3
1.1 PURPOSE 3
1.2 SCOPE 3
1.3 OVERVIEW 3

2 Cryptographic Module Specification 4
2.1 PHYSICAL BOUNDARY 4
2.2 LOGICAL BOUNDARY 4
2.3 MODE OF OPERATION 4

3 Cryptographic Module Ports and Interfaces 7
3.1 PHYSICAL INTERFACES 7
3.2 LOGICAL INTERFACES 8

4 Roles, Services and Authentication 10
4.1 ROLES 10
4.2 SERVICES 11
4.3 AUTHENTICATION 15

5 Physical Security 16

6 Operational Environment 17
6.1 FIPS VS. NON-FIPS MODE 18

7 Cryptographic Key Management 18
7.1 RANDOM NUMBER GENERATORS (RNG) 20
7.2 KEY GENERATION 21
7.3 KEY ESTABLISHMENT 21
7.4 KEY ENTRY / OUTPUT 21
7.5 KEY STORAGE 22
7.6 KEY ZEROIZATION 22

8 Self-Tests 22
8.1 CONDITIONAL SELF-TEST 24

9 Mitigation of Other Attacks 24

1 INTRODUCTION

1.1 PURPOSE

This document specifies the security rules under which the Black Lantern® (BL) Cryptographic Module operates in accordance with NIST FIPS 140-2. The Security Policy is intended to inform individuals and organizations the BL Cryptographic Module's capabilities, protections, and access rights to enable assessment of whether the module will adequately serve the individual or organizational security requirements.

1.2 SCOPE

The security policies described in this document apply to the BL400 installed with BLKSI.2.2.1-FIPS firmware in a limited operational environment. Note that only firmware versions listed on the certificate are CMVP-validated and any others will be out of scope.

1.3 OVERVIEW

The BL Cryptographic Module is designed to be integrated into products that have a requirement to be FIPS 140-2 Security Level 3 certified, with the following breakdown:

Table 1: FIPS 140-2 Security Levels

FIPS 140-2 Section	Security Level
1 – Cryptographic Module Specification	3
2 – Cryptographic Module Ports and Interfaces	3
3 – Roles, Services, and Authentication	3
4 – Finite State Model	3
5 – Physical Security	3
6 – Operational Environment	N/A
7 – Cryptographic Key Management	3
8 – EMI/EMC	3
9 – Self-Tests	3
10 – Design Assurance	3
11 – Mitigation of Other Attacks	N/A

The module is physically enclosed in a security appliance, designed to protect, and secure the module and any pre-loaded applications determined by the integrated products. The version of the BL Cryptographic Module covered by this security policy document contains pre-loaded application firmware, running in a limited non-modifiable operational environment. More information about the operational environment may be found in Section 6.

2 CRYPTOGRAPHIC MODULE SPECIFICATION

2.1 PHYSICAL BOUNDARY

The physical boundary covers the secure enclosure and a subset of internal relevant processing and non-volatile memory components within, in the form of a 1U 19" rack mountable appliance, exclusive of the removable faceplate. This appliance is illustrated in Figure 2-1. However, the optional COM Express daughter card within the enclosure is completely excluded from the requirements of the FIPS 140-2 standard. This daughter card does not process any Critical Security Parameters (CSPs) or any data that would lead to a compromise of the BL Cryptographic Module. It is intended as a supplemental processing component for users of the appliance.

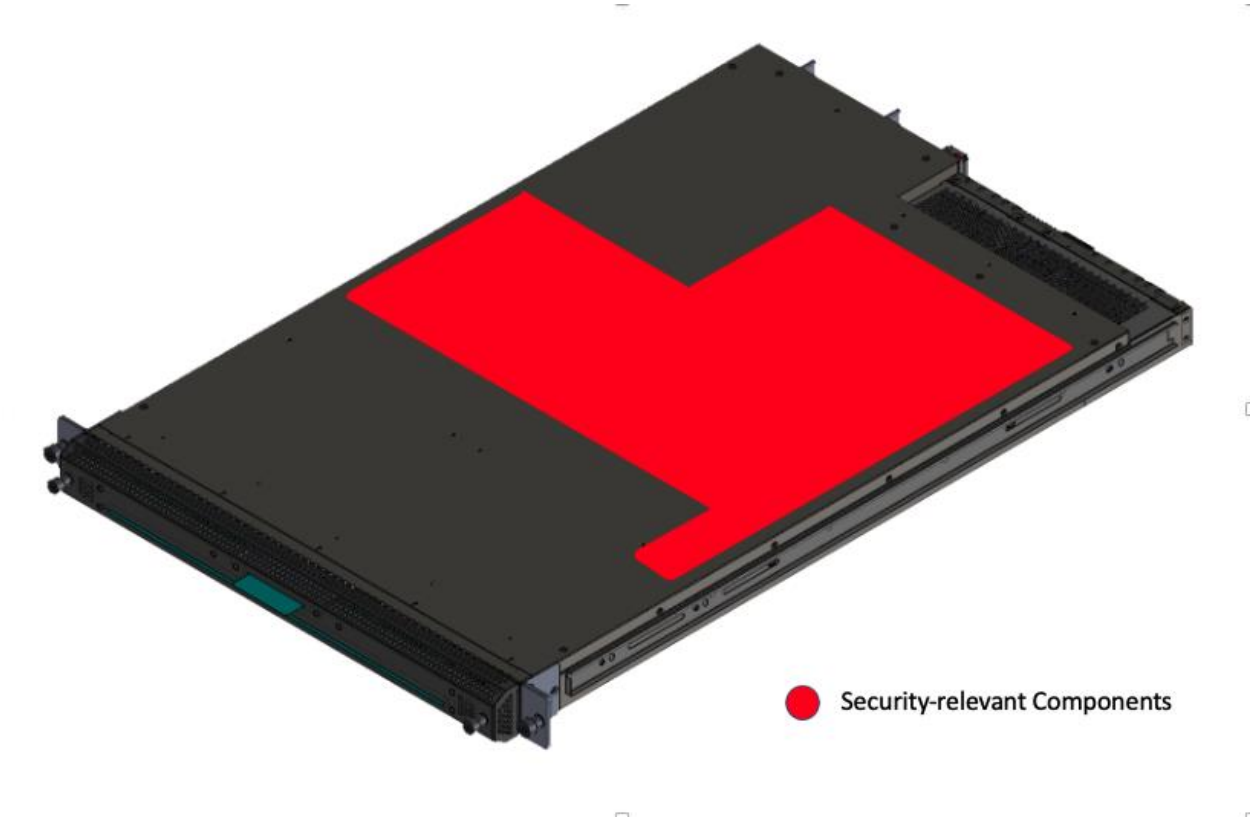

Figure 2-1 – Security-Relevant Components of the Black Lantern Cryptographic Module

2.2 LOGICAL BOUNDARY

Firmware is included in this partition as part of the logical boundary. Within the firmware, there exists the initial boot, the embedded real-time operating system, and the pre-loaded applications, including the hosted applications, specifically the Keyless Signature Infrastructure (KSI®) services.

2.3 MODE OF OPERATION

The BL Cryptographic Module supports a single FIPS-approved mode of operation that the BL Cryptographic Module enters into upon successful completion of power on self-tests. In the

FIPS-approved mode of operation, the BL Cryptographic module supports approved security functions as listed in Table 2 and are accessible with their respective options through their logical interfaces.

Table 2 - Black Lantern Cryptographic Module Approved Security Functions

Approved Security Function	Certificate #
Symmetric Encryption / Decryption	
FIPS 197 AES • SP 800-38A CBC, CTR o Direction: Decrypt, Encrypt o IV Generation: Internal randomly via AES-CTR DRBG o Key Length: 128, 192, 256 • SP 800-38D GCM (used for KTS) o Direction: Decrypt, Encrypt o IV Generation: Internal randomly via AES-CTR DRBG o Key Length: 128, 192, 256	Cert. #A1515
Digital Signatures	
FIPS 186-4 RSA • Key Generation o Modulo: 2048, 3072, 4096 • Signature Generation o Signature Type: PKCS 1.5 o Modulo: 2048, 3072, 4096 o Hash Algorithm: SHA2-256, SHA2-384, SHA2-512 • Signature Verification o Signature Type: PKCS 1.5 o Modulo: 2048, 3072, 4096 o Hash Algorithm: SHA2-256, SHA2-384, SHA2-512	Cert. #A1515
FIPS 186-4 ECDSA • Key Generation o Curve: P-256, P-384, P-521 • Key Verification o Curve: P-256, P-384, P-521 • Signature Generation o Curve: P-256, P-384, P-521 o Hash Algorithm: SHA2-256, SHA2-384, SHA2-512 • Signature Verification o Curve: P-256, P-384, P-521 o Hash Algorithm: SHA2-256, SHA2-384, SHA2-512	Cert. #A1515
Hashing	
FIPS 180-4 SHS • SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Cert. #A1515
Message Authentication	

Approved Security Function	Certificate #
FIPS 198-1 HMAC • HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	Cert. #A1515
Random Number Generation	
SP 800-90B Hardware Entropy Source (ENT (P))	N/A
SP 800-90A Counter DRBG • Mode: AES-128 (self-tests only), AES-192 (self-tests only), AES-256	Cert. #A1515
SP 800-133rev2 Cryptographic Key Generation • Methods: See section 7.2	Vendor Affirmed
Key Derivation	
SP 800-108 KDF CTR • Mac Mode: HMAC-SHA1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 • Fixed Data Order: Before Fixed Data • Counter Length: 32	Cert. #A1515
SP 800-135 KDF TLS[1] • TLS Version: v1.2 • Hash Algorithm: SHA2-256, SHA2-384, SHA2-512	CVL Cert. #A1515
SP800-132 PBKDF (exclusive to password protection) • Iteration Count: 100000, 500000 • HMAC Algorithm: SHA2-256 • Salt Length: 16 bytes • Key Data Length: 32 bytes	Cert. #A1515
Key Agreement	
SP 800-56Arev3 KAS-ECC-SSC • Curve: P-256, P-384, P-521 • Ephemeral Unified: o KAS Role: Initiator, Responder	Cert. #A1515
SP 800-56Arev3 KAS • Curve: P-256, P-384, P-521 • Ephemeral Unified: o KAS Role: Initiator, Responder • Key Derivation: SP 800-135 KDF TLS • Conforms to FIPS 140-3 IG D.8 scenario X1 path 2, combining KAS-SSC Cert. #A1515 and CVL Cert. #A1515	Cert. #A1515
Key Transport	
NIST SP 800-56Brev2 RSADP; Modulus Sizes: 2048	CVL Cert. #A1515

[1] No parts of the TLS protocol, other than the KDF, have been tested by the CAVP and CMVP

Approved Security Function	Certificate #
NIST SP 800-56Brev2 KTS-RSA • Key establishment methodology provides between 112 and 150 bits of encryption strength • KTS-OAEP (Key Transport Using RSA-OAEP) without key confirmation; Modulus Sizes: 2048, 4096	Cert. #A1515

3 CRYPTOGRAPHIC MODULE PORTS AND INTERFACES

3.1 PHYSICAL INTERFACES

The BL Cryptographic Module includes the following physical (non-power) ports/interfaces as shown in Figure 3-1, Figure 3-2, and Figure 3-3.

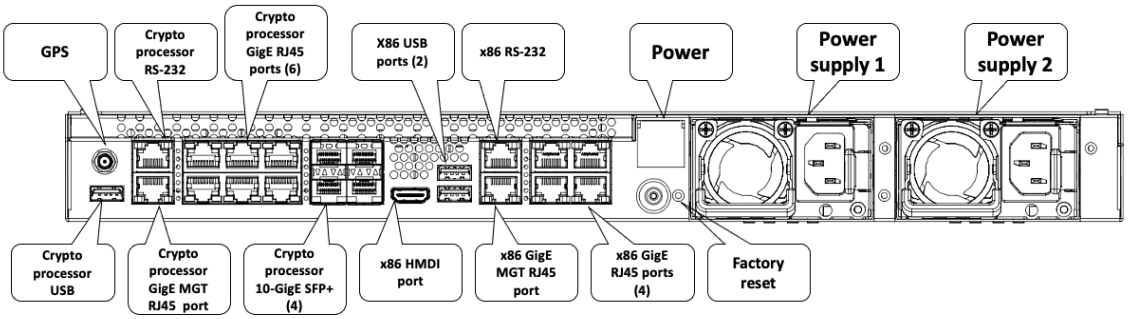

Figure 3-1 Ports and features (rear)

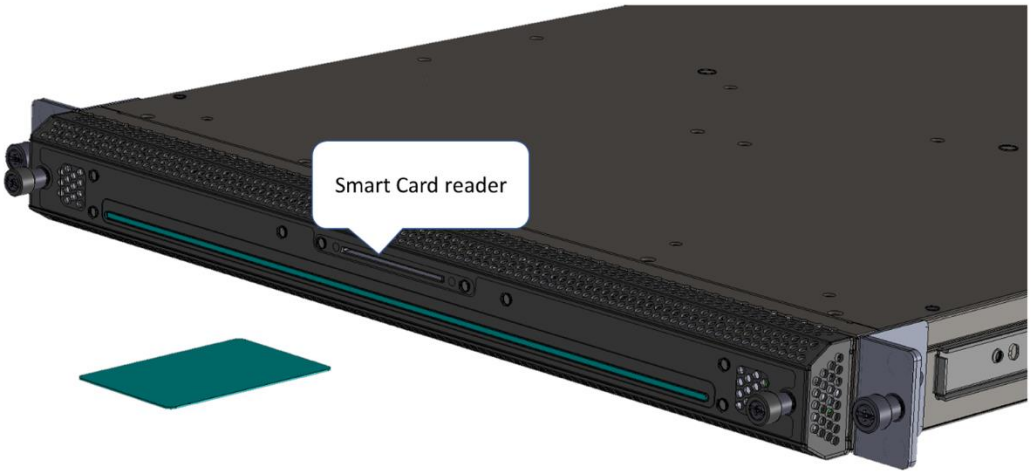

Figure 3-2 Front panel LED bar (removable) and smart card slot

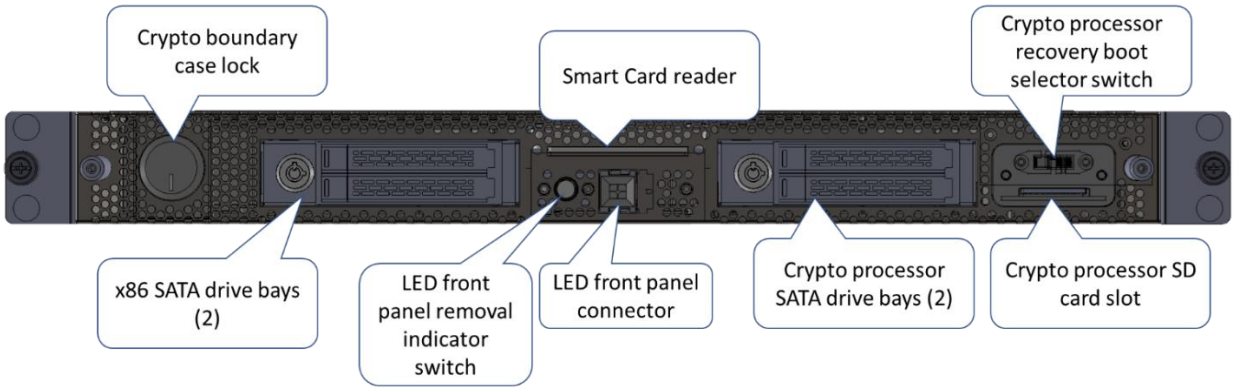

Figure 3-3 Ports and features (front)

Ports (towards left in Figure 3-1) associated with the crypto processor:

- 4 x 10Gb SFP+
- 6 x 1Gb Ethernet RJ45 Copper
- 1 x 1Gb Ethernet Mgmt RJ45 Copper
- 1 x Mgmt RJ45 (RS-232)
- LED
- 1 x USB 2.0 (*Not supported*)
- GPS SMA (*Not supported*)
- Smart Card (*Not supported*)

Ports (towards center in Figure 3-1) associated with the optional COM Express daughter card and as mentioned previously, excluded from the requirements of the FIPS 140-2 standard:

- 4 x 1Gb Ethernet RJ45 Copper
- 1 x 1Gb Ethernet Mgmt RJ45 Copper
- 1 x Mgmt RJ45 (RS-232)
- 2 x USB 3.0
- HDMI

The SFP+ and copper Gigabit Ethernet ports are network interface ports that are configurable and usable by applications via the BL Cryptographic Module's network stack. These ports may be configured to allow for remote user and configuration administration.

The BL Cryptographic Module provides an RJ45 serial port as a console management interface for local administration of the unit. This interface can be accessed using a third-party terminal emulation application from a directly connected PC and must be user authenticated prior to access. This interface implements access to user, configuration, and key management. The key management includes input and output of any plaintext key components, specifically public keys and secret split keys using split procedures, which is limited to this physical port only.

3.2 LOGICAL INTERFACES

The BL Cryptographic Module provides the following logical interfaces:

- Serial Console Command Line Interface (CLI)
- RESTful Interface
- Network Stack

Prior to the startup of Crypto Service, self-tests are always performed prior to servicing any requests. If any self-tests fail, the failed test(s) is immediately logged or displayed in the serial console output interface during the error state before transitioning back to a serviceable state (if allowed).

Crypto Service services each logical interface serially one request at a time, which results in a logical disconnect among the interfaces and inhibits each logical interface from overstepping each other. This ensures that data and control inputs will be logically separated from data and status outputs since each service request will always receive a service response prior to servicing another request. This also ensures operations such as key generation, key entry, or key zeroization will not be interfered with from other requests. In the event of an error, data output will be inhibited while the error state logs or reports the error as status appropriately. Therefore, each logical interface described below can be assured of logical separation as well. However, the exception is periodic self-tests for Crypto Service, which is run concurrently. In this case, mutual exclusion protections have been designed in and implemented to ensure logical disconnect.

Table 3 - Logical and Physical Interface Mapping

	Mgmt RJ45 (RS-232) (1)	**1G RJ45 Ethernet Mgmt Port (1)**	**1G Ethernet RJ45 Ports (6)**	**10G SFP+ Ports (4)**
Serial Console CLI	Data Input/Output Control Input Status Output			
RESTFul Interface		Data Input/Output Control Input Status Output		
Network Stack			Data Input/Output Control Input Status Output	Data Input/Output Control Input Status Output

3.2.1 Serial Console Command Line Interface

The serial console serves as a data input/output, control input, and status output interface for the BL cryptographic module. The terminal provides the ability for administrative users to log in and perform user and key management functions. There can only be a single user logged in at a time, which implies the use of cryptographic services serially. Details of functionality for these users are provided in Section 4.

Specifically, the security administrator and other roles can utilize the control interface to invoke functions such as key generation and key import/export. These functions are described in the command usage located in the User Guide. The usage details outline the separation of control and data input as well as the separation status and data output in the form of usage and parameter option/value descriptions. As mentioned previously, input and output of any plaintext key components are limited to this logical interface implementation only. The serial console provides status information outputs, including any error status, as the module starts up as a result of a reboot command or a power on condition or after invoking a console command.

3.2.2 RESTful Interface

The BL Cryptographic Module provides a RESTful Interface for remote management. Administrators must configure and use this interface over a TLS (trusted and encrypted) channel to manage the module remotely. In addition, the module only processes RESTful API calls from configured authenticated clients. See section 4.3 for details on this authentication.

This interface serves as a data input/output, control input, and status output logical interface. RESTFul API calls are honored serially, so at most, a single request is responded to at a given time, creating logical separation. The APIs are described in the RESTFul sections located in the User Guide. The documentation outlines the separation of control and data input as well as the separation status and data output in the form of endpoint and request/response JSON schema (key/value) descriptions.

3.2.3 Network Stack

The network stack provides a means to enable applications to create logical interfaces to the networking ports at the edge of the module's cryptographic boundary. Specifically, these include the SFP and copper networking physical interfaces. A relevant logical example is the RESTFul interface. Additionally, the networking stack provides a TCP/IP interface via the PCIe to allow application software running on the module's CPU to communicate with application software running on the optional COM Express module.

This interface serves as a data input/output, control input, and status output logical interface. TCP/IP protocol ensures a logical separation across these interfaces when applied.

4 ROLES, SERVICES AND AUTHENTICATION

This section describes the various functional roles that operators of the BL Cryptographic Module can undertake, the various services those roles are authorized to perform as well as the authentication mechanisms used for authenticating operators.

4.1 ROLES

The BL Cryptographic Module supports the following roles:

Table 4 – Supported Roles

Role	Description
Security Administrator	User management, device and security configuration management, module provisioning, firmware update, and crypto/key management.
Network Administrator	Network configuration management.
Application Administrator	Configuration management for hosted services.
Recovery Agent	Exclusive secret key split or share owner for the sake of unencrypted key backup and recovery.
Internal Services	Internal services that are available to the applications running on the module.

For the remainder of this document, please note the Security Administrator role is equivalent to the Crypto Officer role in addition to other responsibilities detailed in Section 4.2.

Operators under these roles can utilize the serial console to log in (one at a time) to perform services. Similarly, operators may also access the BL Cryptographic Module through the remote RESTful interface for remote administration functions.

4.2 SERVICES

Services described in this section are considered FIPS 140-2 Approved. The usage of FIPS 140-2 Approved Security Functions are referenced in Table 2.

Table 5 – Role-based Services

Service	Critical Security Parameters (read, write)	Authorized Role				
		Security Admin	Network Admin	Application Admin	Recovery Agent	Internal Services
Add role to user	Operator Password (read) Storage Keys (read)	X				
Add new user	Operator Password (read, write) Storage Keys (read)	X				
Set or display the security banner	Storage Keys (read)	X				
Clear current screen	N/A	X	X	X	X	
Delete application configuration	Storage Keys (read)			X		

Remove role from user	Operator Password (read) Storage Keys (read)	X				
Delete user	Operator Password (read) Storage Keys (read)	X				
Login	Operator Password (read)	X	X	X	X	
Logout	N/A	X	X	X	X	
Export (print) data files	BL Authentication Keys (read) User Keys (read)	X			X	
Generate certificate signing request	User Keys (read)	X				
Generate keys	User Keys (write)	X				
Get application configuration	Storage Keys (read)			X		
Get certificate information	CA Certificates (read) Storage Keys (read) TLS Certificate (read)	X				
Get device configuration	Storage Keys (read)	X	X	X		
Get status	N/A	X	X	X		
Print current UTC time	N/A	X	X	X	X	
Get user information	Storage Keys (read)	X				
Help menu	N/A	X	X	X	X	
Command history buffer	N/A	X	X	X	X	
Get and set network configuration	Storage Keys (read)		X			

Import data files	BL Authentication Keys (read) CA Certificates (write) TLS Certificate (write) TLS Private Key (write) User Keys (read)	X			X	
Enforces key ceremony for backup and recovery	Storage Keys (read)	X			X	
List directory contents	N/A	X		X		
Modify user	Operator Password (read) Storage Keys (read)	X				
Change password of user	Operator Password (read, write) Storage Keys (read)	X	X	X	X	
Ping the specified host	N/A	X	X	X	X	
Reboot the system	Storage Keys (read)	X				
Remove directories or files	N/A	X		X		
Get and set route table	Storage Keys (read)		X			
Manage hosted (application) services	N/A			X		
Set application configuration	Storage Keys (read)			X		
Set configuration settings	Storage Keys (read)	X	X			
Set system time	N/A		X			
Shutdown the system	Storage Keys (read)	X				

Update system with firmware	Depot Authentication Public Key (read) Depot System Keys (read)	X				
View local log	N/A	X				
Print the current user	N/A	X	X	X	X	
TLS communication	CA Certificates (read) TLS Certificate (read) TLS Private Key (read)					X
Key derivation	Depot System Keys (read)					X
Symmetric encryption/decryption	Depot System Keys (read)					X
Asymmetric encryption/decryption	User Keys (read)					X
Signature generation	BL Authentication Keys (read)					X
Signature verification	Depot Authentication Public Key (read) BL Authentication Keys (read)					X
Hash generation	N/A					X
MAC generation	User Keys (read)					X
MAC verification	User Keys (read)					X
Self-test	N/A					X
Key zeroization	All volatile Keys (write) Zeroizable Key (write)	X				X

4.3 AUTHENTICATION

Externally, the BL Cryptographic Module provides a local serial console and a RESTful API as mechanisms to access its services. Services are limited to administrators and recovery agents and are available only after they have provided acceptable user identification and authentication data to the module.

Internally, the BL Cryptographic Module provides cryptographic services to the applications which have been authenticated by virtue of being bundled as part of the signed firmware image, which utilizes a signature that provides 256 bits of security strength (which equates to a 1 in 2^256 chance of randomly being able to forge a valid signature)

4.3.1 Serial Console Interface Authentication

The BL Cryptographic Module supports the local (i.e., on device) definition of operators using identity-based authentication with individual usernames and passwords. These operators are associated with role(s) set by the security admin, enabling specific services for each.

When an operator is authenticated at the local console, no information about the authentication data (i.e., password) is echoed to the user. These passwords are secured using PBKDF2 with a random nonce or salt value and always stored in the module as hashed and encrypted, never exposing the password in plaintext during authentication.

Password policy enforces a minimum length of 8 characters and is configurable to increase. Passwords can be composed of any combination of upper (26) and lower (26) case letters, numbers (10), and the following special characters (17): !; @; #; $; %; ^; &; *; (;); _; ?; <; >; .; ~; and |. Therefore, the probability for a successful random access is 1 in 79^8, which is significantly less than 1 in a 1,000,000. In addition, rate limiting exists in the form of a configurable max authentication attempts setting at 5 prior to indefinite account disabling, in which only a security administrator may re-enable. This bound will ensure the probability of a successful random access within a 60-second span is less than 1 in 100,000.

4.3.2 RESTful Interface Authentication

The BL Cryptographic Module supports the use of X.509v3 certificates for TLS authentication and also supports certificate revocation checking using OCSP mechanism as specified in RFC 2560. It will not accept a certificate if it is unable to establish a connection or determine the certificate’s validity.

The remote connection is established using TLS v1.2, in compliance with RFC 5246 and compatible with cipher suites referenced in SP 800-52rev2, Section 3.3.1, to support secure path and channel communications. Remote management TLS connections are mutually authenticated (or two-way TLS), meaning the remote client will supply its own certificate (or identity) to be validated and authorized against a configured list of authorized clients within the module. This mechanism achieves identity-based authentication from a remote perspective. Note that communication with remote management clients utilizes HTTP over TLS.

The following cipher suites are supported to establish a trusted path/channel:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

The weakest among the cipher suites supported is RSA 2048. In this case, the security strength is 112 bits. Therefore, the probability for a successful random access is 1 in 2^112, which is significantly less than 1 in 1,000,000. In addition, rate limiting exists in the form of a single 1Gb ethernet interface processing each TLS connection serially with a minimum connection time of 100 milliseconds. This bound will ensure the probability of a successful random access, within a 60-second span, is less than 1 in 100,000.

With respect to TLS session keys from the supported cipher suites listed earlier, a couple of remarks shall be noted:

- In accordance with RFC 5246, when the nonce_explicit part of the IV exhausts the maximum number of possible values (e.g. 64-bit counter) for a given AES GCM session key, the client or server encountering this condition will attempt to establish a new TLS session key.
- TLS session keys are ephemeral and any power loss during an existing connection would require the TLS connection to be re-established and therefore, invoke a regeneration of the AES GCM session key.

5 PHYSICAL SECURITY

5.1.1 Description

The BL Cryptographic Module is fully contained within a metal enclosure. A removable lid is the only access to the crypto area. The lid is secured by a pick-resistant lock, and factory-applied tamper evident seals are placed over a few seams where the lid interfaces with the enclosure (Figure 5-1). Note that only one of the two mechanisms (either the pick-resistant lock or the tamper evident seals) is required, thus per FIPS 140-2 TE.05.50.01 only the pick-resistant lock was tested. Removal of the lid will trigger a zeroization of the module’s cryptographic keys.

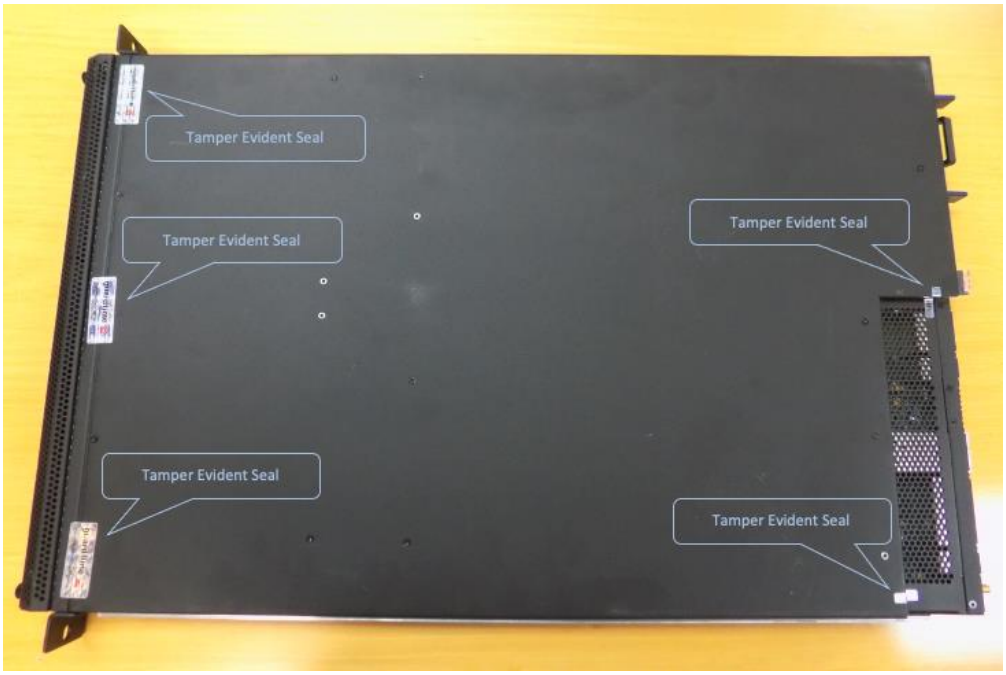

Figure 5-1 Tamper Evident Seal Locations

5.1.2 Maintaining physical security

The following list contains recommended actions to help preserve the security of the BL Cryptographic Module.

- Periodically inspect the device for signs of damage, intrusion, or tamper.
- Periodically inspect the tamper evident seals for evidence that they have been removed, cut or otherwise tampered with. Contact Guardtime Federal immediately if any tampering is observed to determine extent of tamper and further instructions.
- The case lock key (if delivered) should be stored in a secure location only accessible to those with proper authorization.
- The cryptographic key store is battery backed by an internal non-user serviceable rechargeable battery. The battery has been designed to provide enough power to retain the keys for months at a time when the unit is disconnected from AC power. As the battery ages the amount of time it can retain the cryptographic keys may degrade. In order to prevent potential loss of cryptographic keys it is recommended that the BL Cryptographic Module always be plugged into AC power.

6 OPERATIONAL ENVIRONMENT

The BL Cryptographic Module is designed to operate as a cryptographic module within a security appliance that may operate in a networked environment. The module implements a real-time operating system where applications are built-into an operating system monolithic image. The pre-loaded applications, as first mentioned in the logical boundary, leverage and integrate with the BL Cryptographic Module's cryptographic services directly via static library or in a

client-server architecture, while executing on the BL Cryptographic Module's processor. The server application acts as the single user providing cryptographic services to multiple clients.

Since hosted applications are required to be pre-loaded, products integrating the BL Cryptographic Module will need to build in the applications prior to delivering the product to end-users. The BL Cryptographic Module does not provide the ability for end-users to uninstall or install any other applications, outside of a firmware upgrade to the module, resulting in a non-modifiable and limited operating environment.

All cryptographic services are executed on the embedded module's processor out of the attached RAM. The cryptographic services firmware is stored encrypted and digitally signed in non-volatile memory. This firmware gets securely loaded by the boot firmware, which is also stored digitally signed in non-volatile memory.

The BL Cryptographic Module operating system utilizes features of the architecture to provide memory isolation between individual applications as well as the kernel. Applications interface with the cryptographic services through the cryptographic services client library, which uses inter-process communications to communicate with the cryptographic services implemented in a separated memory address space.

6.1 FIPS VS. NON-FIPS MODE

The BL Cryptographic Module is statically set in FIPS mode at build time. There exists no configuration to dynamically set the module to non-FIPS mode. Only FIPS-approved security functions will be allowed when in FIPS mode.

To determine when in FIPS mode, upon successful login, the serial console shall indicate with text that the module is set in FIPS mode. When logged in, the administrator may alternatively use the "getstatus" serial console command to actively query the module's FIPS mode status.

7 CRYPTOGRAPHIC KEY MANAGEMENT

The BL Cryptographic Module manages cryptographic keys and Critical Security Parameters (CSPs) in support of cryptographic services. This section specifies all cryptographic keys and CSPs managed by the BL Cryptographic Module along with how each are protected against unauthorized disclosure, modification, and substitution.

Table 6 – Summary of keys and CSPs

Key / CSP	CSP Type	Usage	Generation	Input / Output
BL Authentication Keys	EC secp521r1	Signs and verifies keys or data on import and export.	FIPS PUB 186-4, Appendix B.4	Loaded at the Depot. No output.

Depot Authentication Public Key	EC secp521r1	Verifies data generated by the Depot.	FIPS PUB 186-4, Appendix B.4	Loaded at the Depot. No output.
Depot System Keys	AES-GCM 256	Encrypts other system keys and data from Depot.	NIST SP 800-90A AES-CTR DRBG, SP 800-108 KDF CTR	Loaded at the Depot. No output.
DRBG CSPs	SP 800-90A AES-CTR DRBG entropy input (256), seed (256, 320, 384), V (128), and Key (128, 192, 256) values	Random Bit Generation.	The entropy input is generated by the module's ENT. The seed, V, and Key values are produced in accordance with the SP 800-90A specification	No input / output.
CA Certificates	EC (secp256r1, secp384r1, secp521r1) or RSA (2048, 3072, 4096)	TLS verification with remote clients and servers.	Externally generated by operator.	Input and output in plaintext.
Operator Password	8-32 alphanumeric or special characters	Login password for the serial console interface.	Externally generated by operator.	Input in plaintext. No output.
TLS Certificate	EC (secp256r1, secp384r1, secp521r1) or RSA (2048, 3072, 4096)	TLS communication with remote clients and servers.	External to the BL Cryptographic Module.	Input and output in plaintext.
TLS Ephemeral Public Key	EC (secp256r1, secp384r1, secp521r1)	Facilitates TLS key exchange with computation of pre-master secret.	FIPS PUB 186-4, Appendix B.3, B.4	Input and output in plaintext.
TLS Ephemeral Private Key	EC (secp256r1, secp384r1, secp521r1)	Facilitates TLS key exchange with computation of pre-master secret.	FIPS PUB 186-4, Appendix B.3, B.4	No input / output.
TLS Master Secret	48 bytes	Derives session keys for TLS.	NIST SP 800-135 TLS 1.2 KDF	No input / output.
TLS Pre-Master Secret	EC point x-coordinate as shared secret from ECDHE key exchange method	Derives master secret for TLS.	NIST SP 800-56Arev3	No input / output.

TLS Private Key	EC (secp256r1, secp384r1, secp521r1) or RSA (2048, 3072, 4096)	TLS communication with remote clients and servers.	FIPS PUB 186-4, Appendix B.3, B.4	No input / output.
TLS Session Keys	AES-GCM 256 or HMAC-SHA-384	Encrypts or ensures integrity of client and server messages over TLS.	NIST SP 800-135 TLS 1.2 KDF	No input / output.
Storage Keys	AES-GCM 256	Encrypts user data at-rest on the BL Cryptographic Module.	NIST SP 800-90A AES-CTR DRBG	No input / output.
User Keys	AES-GCM (128, 192, 256) or EC (secp256r1, secp384r1, secp521r1) or RSA (2048, 4096)	Encrypts user keys or data for export or service usage.	NIST SP 800-90A AES-CTR DRBG or FIPS PUB 186-4, Appendix B.3, B.4	Public keys input / output in plaintext but verified, Secret keys input / output encrypted or in plaintext using shared secret procedures.
Zeroizable Key	AES-GCM 256	Encrypts Storage Keys.	NIST SP 800-90A AES-CTR DRBG	Input and output encrypted.

7.1 RANDOM NUMBER GENERATORS (RNG)

The BL Cryptographic Module utilizes a non-deterministic entropy source to seed the implementation of the NIST SP 800-90A AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-57 Part 1 Rev. 5, Table 2: “Comparable strengths”. The implementation uses one entropy source, which accumulates entropy from one hardware-based noise source to take advantage of 512 bits of seeding entropy at a time.

Although the AES-CTR DRBG instance supports multiple key sizes, it is not configurable by the operator but statically set at AES-256 with the derivation function enabled.

7.2 KEY GENERATION

For symmetric cryptographic key generation, keys are generated using unmodified output directly from the AES-CTR DRBG.

For asymmetric cryptographic key pair generation, the same DRBG is used for seeding under the following approved key generation schemes:

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;
- ECC schemes using "NIST curves" [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;

7.3 KEY ESTABLISHMENT

For key establishment, the BL Cryptographic Module utilizes Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56Arev3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography".

7.4 KEY ENTRY / OUTPUT

For symmetric or asymmetric private key entry (import) / output (export), the serial console interface is the logical interface supported in this manual method.

During export key wrapping, the operator will specify a key (symmetric or asymmetric public) to encrypt the specified target key for transport. Upon export, a signature is also attached to the wrapped key, which is a Base64-encoded output to the serial console interface.

The following algorithms are supported for key wrapping:

- AES-GCM
- RSA-OAEP

Inversely, during import through the serial console interface, the wrapped key is always authenticated prior to decryption.

Note that public key import and export do not require key wrapping (encryption). However, they are always authenticated during import.

Importing/Exporting unencrypted symmetric key splits is also supported, which involves specific split procedures detailed in the User Guide. This Key Ceremony is a means for key backup for disaster-recovery scenarios. Performing the Key Ceremony is a tightly controlled process using dedicated, direct-connected, and non-networked laptops for each split key to enforce security within an isolated trusted path. It involves individually assigned roles (Security Admin and Recovery Agents) for administrators that collectively share in the responsibilities of key generation, key combining, and administering permissions to import and/or export a designated secret split key, exclusive to each recovery agent and separately authenticated via the serial

console interface. Also, note that each split key requires an authentication step prior to importing into the BL Cryptographic Module. Once the Key Ceremony is closed, these responsibilities are permanently locked from administrators of the module.

7.5 KEY STORAGE

All keys stored in non-volatile memory are always stored encrypted at-rest. Keys in volatile memory are unencrypted but zeroized typically when the security function completes and no longer requires the key or when the BL Cryptographic Module powers off or reboots.

7.6 KEY ZEROIZATION

Key zeroization in volatile memory occurs when the BL Cryptographic Module powers off or reboots.

Upon detection of a critical tamper event (e.g. cover panel of chassis removed), the Zeroizable Key will be zeroized and the key store holding all keys in volatile memory will be shut down immediately, thereby zeroizing all keys in volatile memory. This effectively limits operators from using cryptographic services against any CSPs (Critical Security Parameters).

8 SELF-TESTS

The module Power-On Self-Tests (POST) confirm the firmware integrity, check the random number generator, and test each of the implemented cryptographic algorithms. While the module is running POST, all logical interfaces are disabled until the successful completion of the self-tests. POST are required for the module and will not provide any cryptographic services until fully successful. The POST are performed in two groups: 1. Self-tests to verify firmware integrity functionality, 2. Self-tests using Known Answer Tests (KAT) to validate security functions.

The self-tests are initiated at power on and do not require input from an operator. If a self-test fails the module will go into an error state and the option to reboot the module will be presented, this will clear the current results and rerun the self-tests. If the error persists through a reboot the user should contact GTF to determine the next course of action.

Table 7 – Self-tests Group 1

Group Test 1	**When Performed**	**Error Indicator**
Boot loader performs an RSA 4096 SHA-256 signature verification of itself	Power-on	Error output and module halt
Boot loader performs an ECDSA 521 SHA-256 signature verification prior to firmware start	Power-on	Error output and module halt

Table 8 – Self-tests Group 2

Group Test 2	When Performed	Error Indicator
ctrDRBG KAT (Mode: Instantiate, Generate, Reseed; Key Len: AES-128, AES-192, AES-256)	Power-on	Error output and Crypto Service degradation
AES KAT (Mode: CBC, CTR, GCM; Key Len: 128, 192, 256)	Power-on	Error output and Crypto Service degradation
ECDSA KAT (Mode: Key Generation, Public Key Verification, Signature Generation, Signature Verification; Curve: secp256r1, secp384r1, and secp521r1)	Power-on	Error output and Crypto Service degradation
SHA KAT (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Power-on	Error output and Crypto Service degradation
HMAC KAT (HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512)	Power-on	Error output and Crypto Service degradation
KAS ECC SSC ephemeralUnified SP800-56Ar3 KAT (Curve: secp256r1, secp384r1, and secp521r1)	Power-on	Error output and Crypto Service degradation
KTS IFC KTS-OAEP-basic SP800-56Br2 KAT (Hash: SHA2-224, SHA2-256, SHA2-384, SHA2-512; Modulo: 2048, 4096)	Power-on	Error output and Crypto Service degradation
RSA FIPS186-2 KAT (Mode: Signature Verification; Hash: SHA2-256, SHA2-384, SHA2-512; Modulo: 2048, 3072, 4096)	Power-on	Error output and Crypto Service degradation
RSA FIPS186-4 KAT (Mode: Key Generation, Signature Generation, Signature Verification; Hash: SHA2-256, SHA2-384, SHA2-512; Modulo: 2048, 3072, 4096)	Power-on	Error output and Crypto Service degradation
KDF CTR KAT (HMAC-SHA1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512)	Power-on	Error output and Crypto Service degradation
PBKDF KAT (HMAC-SHA2-256)	Power-on	Error output and Crypto Service degradation
TLS v1.2 KDF-Components KAT (Hash: SHA2-256, SHA2-384, SHA2-512; Key Block Len: 1024)	Power-on	Error output and Crypto Service degradation
Startup Tests on the module's ENT (RNG4.2), executing the Health Tests on 1024 samples	Power-on	Error output and module halt

8.1 CONDITIONAL SELF-TEST

The module automatically performs conditional self-tests based on the module operation. These self-tests do not require operator input to initiate.

Table 9 – Conditional Self-tests

Test	When Performed	Error Indicator
Long Runs Test (Repetition Count Test) on the module's ENT (RNG4.2)	Conditional	Error output and random number discarded
Monobit Test (variation of Adaptive Proportion Test) on the module's ENT (RNG4.2)	Conditional	Error output and random number discarded
DRBG Health Tests	Periodic	Error output and random number discarded
RSA (Pair-wise consistency test)	Conditional	Error output and key pair discarded
ECC (Pair-wise consistency test)	Conditional	Error output and key pair discarded
Firmware update verification test	On firmware update	Error output and firmware rejected

9 MITIGATION OF OTHER ATTACKS

This security policy makes no claims of mitigation of other attacks.