National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Guardtime Federal Black Lantern® BL300 Series and BL400 with BLKSI.2.2.1-FIPS

Report Number: CCEVS-VR-11287-2022
Dated: 9 September 2022
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
Jenn Dotson
Sheldon Durrant
Lisa Mitchell
Lori Saren

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Guardtime Federal Black Lantern® BL300 Series and BL400 with BLKSI.2.2.1-FIPS consisting of Black Lantern® BL300-B2, BL300-C2, and BL400-A1 appliances with firmware version BLKSI.2.2.1-FIPS (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation of Guardtime Federal Black Lantern® BL300 Series and BL400 with BLKSI.2.2.1-FIPS was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in September 2022. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, release 5 ([1], [2], [3], [4], and assurance activities specified in *Evaluation Activities for Network Device cPP*, Version 2.2, December 2019 [6]. The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The TOE is a network device appliance intended to mitigate both remote and physical attacks against a customer infrastructure and applications. Black Lantern includes a Keyless Signature Infrastructure (KSI®) gateway and extender that provides implementation of KSI-based data assurance. The KSI gateway and extender functionality of Black Lantern is not covered by the *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 ([5]) and therefore is not evaluated. The focus of this evaluation is on the TOE functionality supporting the claims in this Protection Profile (PP).

The security functionality specified in this PP includes protection of communications between the TOE and external IT entities, identification and authentication of administrators, auditing of security-relevant events, ability to verify the source and integrity of updates to the TOE, and use of NIST-validated cryptographic mechanisms.

The Leidos evaluation team determined that the TOE is conformant to the claimed PP. The TOE, when configured as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in *Guardtime Federal Black Lantern® BL300 Series and BL400 with BLKSI.2.2.1-FIPS Security Target*, Version 1.0, 1 September 2022 ([8]). The information in this VR is largely derived from the Assurance Activities Report (AAR) ([10]) and associated test report produced by the Leidos evaluation team ([11]).

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test report. The validation team found that the evaluation showed that the TOE satisfies all of the security functional and assurance requirements stated in [ST]. The evaluation also showed that the TOE is conformant to the claimed PP, and that the assurance activities specified in [6] had been performed appropriately. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the Evaluation Technical Report ([9]) are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product and its evaluation.

Table 1: Evaluation Details

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluated Product:	Guardtime Federal Black Lantern® BL300 Series and BL400 with BLKSI.2.2.1-FIPS, specifically consisting of BL300-B2, BL300-C2, and BL400-A1 appliances with firmware version BLKSI.2.2.1-FIPS
Sponsor & Developer:	Guardtime Federal 1700 Diagonal Road, Suite 320 Alexandria, VA 22314
CCTL:	Leidos 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	September 8, 2022
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
CEM:	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.
Protection Profiles:	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020
Disclaimer:	The information contained in this Validation Report is not an endorsement either expressed or implied of the TOE
Evaluation Personnel:	Leidos: Pascal Patin, Dawn Campbell, Allen Sant
Validation Personnel:	Paul Bicknell, Jenn Dotson, Sheldon Durrant, Lisa Mitchell, Lori Saren

3 Assumptions and Clarification of Scope

3.1 Assumptions

The Security Problem Definition, including the assumptions, can be found in the following document:

- *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020

That information has not been reproduced here and CPP_ND_V2.2E should be consulted if there is interest in that material.

3.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_ND_V2.2E as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in *Evaluation Activities for network Device cPP*, December 2019, Version 2.2 and performed by the evaluation team).

This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.

The evaluation of security functionality of the product was limited to the functionality specified in the ST. Any additional security related functional capabilities of the product were not covered by this evaluation.

This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

The TOE appliances consist of firmware and hardware and do not rely on the operational environment for any supporting security functionality.

The TOE must be installed, configured and managed as described in the *Guardtime Federal Black Lantern Guidance Documentation*, Version 1.1 included in the evaluated configuration.

4 Architectural Information

The TOE is identified as the Guardtime Federal Black Lantern® BL300 Series and BL400 with BLKSI.2.2.1-FIPS consisting of Black Lantern BL300-B2, BL300-C2, and BL400-A1 appliances with firmware version BLKSI.2.2.1-FIPS from Guardtime Federal.

The TOE is a network appliance designed to mitigate both remote and local physical attacks against a customer's infrastructure and applications. Black Lantern incorporates a Keyless Signature Infrastructure (KSI) gateway and extender, allowing for secure implementation of KSI-based data assurance and cybersecurity solutions with built-in active anti-tamper measures. Note that the KSI gateway and extender functionality of Black Lantern and its ability to support KSI-based data assurance and cybersecurity solutions with built-in active anti-tamper measures has not been evaluated.

For the purpose of this evaluation, the TOE is treated as a network device offering NIST validated cryptographic functions, security auditing, secure administration, trusted updates, self-tests, and secure connections to other servers (e.g., to export audit records), protected using HTTPS/TLS and SSH.

Cryptographic functionality is performed by Guardtime Federal's Cryptographic Support Library (CSL) Direct. The module's FIPS-Approved cryptographic algorithms have obtained CAVP certificates.

The TOE audits security relevant events, stores audit records locally, and can be configured to forward its audit records to an external syslog server in the network environment over a TLS-protected connection. An administrator can configure the TOE to solicit time from an NTP server, and alternatively the administrator can manually set the TOE's time.

The TOE supports a local administration capability via an RS-232 serial interface that provides access to its Serial Console Interface (SCI). The SCI presents a command line interface (CLI). Suitably privileged administrative users can perform all management commands and configuration of the TOE via this interface.

The TOE also supports a remote administration capability via a RESTful interface that enables an administrator to submit management requests to the TOE via calls to the TOE's RESTful API. All communication via the RESTful API is protected using HTTPS.

The TOE implements a local password-based authentication mechanism to control both local and remote access to the TOE.

Administrators are able to query the current running version of the TOE firmware and to initiate firmware updates. The vendor provides TOE updates as encrypted and digitally signed packages. The TOE uses 256 bit AES to decrypt the image and ECDSA with NIST curve P-521 to verify the digital signature.

The TOE implements a battery of Power On Self-Tests (POSTs) that ensure the integrity and correct operation of the TOE.

5 Security Policy

The TOE enforces the following security policies as described in the Security Target (ST).

Note: Much of the description of the security policy has been derived from the ST and Evaluation Technical Report (ETR).

5.1 Security Audit

The TOE is able to generate audit records of security relevant events. The TOE stores audit records locally and can also be configured to send the audit records to an external syslog server over a protected communication channel. The TOE protects locally stored audit records from unauthorized modification and deletion. By default, the TOE overwrites the oldest locally stored audit records and maintains a count of the number of overwritten records if space for storing newly generated audit records is exhausted. Alternatively, the administrator can configure the TOE to drop all new records and keep a counter of the audit records dropped when the local storage is full. In addition, the TOE generates a warning to inform the administrator before the audit trail exceeds the local audit storage capacity.

5.2 Cryptographic Support

The TOE includes Guardtime Federal's Cryptographic Support Library (CSL) Direct v2.0.0 cryptographic module, which provides the following CAVP-certified cryptographic services: random bit generation; asymmetric cryptographic key pair generation; key establishment; symmetric data encryption and decryption; digital signature generation and verification; cryptographic hashing; and keyed-hash message authentication. These services support implementation of higher-level cryptographic protocols, specifically TLS and HTTPS.

5.3 Identification and Authentication

The TOE requires all users to be successfully identified and authenticated prior to accessing its security management functions and other capabilities.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords. When a user is authenticated at the SCI, no information about the authentication data (i.e., password) is echoed to the user. Passwords can be composed of any combination of upper and lower case letters, numbers, and the following special characters: !; @; #; $; %; ^; &; *; (;); _; ?; <; >; ,; .; ~; and |.

The TOE responds to consecutive failures to authenticate remote password-based login attempts. The TOE validates credentials in the HTTPS header of RESTful requests against a local user account and keeps a count of consecutive failed authentication attempts for each configured user. If the number of consecutive failed authentication attempts reaches the configured value for allowed failed attempts, the local account will be disabled and subject to be re-enabled by a Security Admin user. All users are subject to lockout following consecutive failed remote authentication attempts, but users with the Security Admin role can never be locked out of the SCI.

The TOE supports the use of X.509v3 certificates for TLS authentication and also supports certificate revocation checking using OCSP. The TOE will not accept a certificate if it is unable to establish a connection in order to determine the certificate's validity.

5.4 Security Management

The TOE supports local and remote security administration via the SCI and the RESTful API respectively. The TOE supports the following two administrator roles that together provide the capabilities of the Security Administrator role as defined in CPP_ND_V2.2E - Security Admin and Network Admin.
The TOE provides the security management functions necessary to configure and administer its security capabilities. These capabilities include configuring a login access banner, configuring a local session inactivity time limit before session termination, configuring the audit function, including export of audit

records to an external audit server, setting the system date and time and configuring NTP, performing firmware updates, and managing X.509 certificates.

5.5 Protection of the TSF

The TOE protects sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator.

The TOE provides reliable time stamps for its own use and can be configured to synchronize its time via NTP.

The TOE provides a trusted means for determining the current running version of its firmware and to update its firmware. The TOE verifies the integrity of TOE updates using a digital signature.

The TOE implements various self-tests that execute during the power-on and start up sequence, including cryptographic known answer tests that verify the correct operation of the TOE's cryptographic functions.

5.6 TOE Access

The TOE will terminate local interactive sessions at the SCI after a configurable period of inactivity. The default time-out value is 300 minutes and this can be configured by a user with the Security Admin or Network Admin role.

The use of the RESTful API for remote security management means there is no concept of an interactive session for remote administrators—each request to the API is a self-contained, identified and authenticated request. As such, TSF-initiated termination of remote administrative sessions is deemed to occur immediately after the TOE services the request.

The TOE provides the capability for users to terminate their own local sessions by logging out of the TOE. For user-initiated termination of remote interactive sessions via the RESTful API, the interactive session is terminated immediately after the request is submitted to the interface.

The TOE can be configured to display an advisory and consent warning message before establishing a user session.

5.7 Trusted Path/Channels

The TOE protects communications with remote administrators using HTTPS (for access to the REST API).

The TOE is able to protect transmission of audit records to an external audit server using TLS.

6 Documentation

Guardtime Federal provides documentation for the end users of the Black Lantern TOE, for installation, configuration and use of the TOE. The following document was specifically examined in the context of the evaluation: *Guardtime Federal Black Lantern Guidance Documentation*, Version 1.1, September 1, 2022 ([11]).

7 Evaluated Configuration

The Target of Evaluation (TOE) is identified as the Guardtime Federal Black Lantern® BL300 Series and BL400 with BLKSI.2.2.1-FIPS consisting of Black Lantern BL300-B2, BL300-C2, and BL400-A1 appliances with firmware version BLKSI.2.2.1-FIPS developed by Guardtime Federal. Specifically, the BL300-B2 appliance was used for testing.

The TOE is installed and configured according to the product installation guidance identified in Section 6. No additional configuration is necessary to run the TOE in FIPS mode.

7.1 Excluded Functionality

All product functionality that is not claimed by the Security Target as part of achieving exact conformance to the NDcPP is excluded from the evaluation scope. This includes the KSI gateway and extender functionality of Black Lantern and its ability to support KSI-based data assurance.

8 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the proprietary Guardtime Federal Black Lantern® BL300 Series and BL400 with BLKSI.2.2.1-FIPS Common Criteria Test Report and Procedures For Network Device collaborative PP Version 2.2e, Version 1.1, August 30, 2022 (TR), as characterized in the publicly available Assurance Activities Report (AAR).

The evaluation team devised a test plan based on the Test Assurance Activities specified in [cPPND-SD]. The test plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the test plan and documented the results in the team test report identified above.

Testing of the TOE was performed at the Leidos Accredited Testing and Evaluation Lab located in Columbia, Maryland from March 29, 2022 to July 7, 2022, with additional testing performed on August 29, 2022 to support check-out. The TR, in Section 3, lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *collaborative Protection Profile for Network Devices* were fulfilled.

8.1 Test Configuration

The evaluated configuration of the TOE consists of the Guardtime Federal Black Lantern® BL300 Series and BL400 with BLKSI.2.2.1-FIPS consisting of Black Lantern BL300-B2, BL300-C2, and BL400-A1 appliances with firmware version BLKSI.2.2.1-FIPS developed by Guardtime Federal.

Each appliance contains an NXP T4240r2 QorIQ, 12 Dual Cores 64-bit Power Architecture (microarchitecture), 1667 MHz with SEC processor.

The TOE models differ only in terms of number of external network ports and storage capacity. All models use the same firmware image files and provide equivalent security-relevant functionality. There are no security relevant differences between the appliance models.

The BL300-B2 TOE appliance was tested in the evaluated configuration. Since the TOE models use the same firmware image files and provide equivalent security-relevant functionality, they are considered equivalent.

The TOE must be configured in accordance with the *Guardtime Federal Black Lantern Guidance Documentation*, Version 1.1, September 1, 2022.

Per Policy Letter #22, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

8.2 Vulnerability Analysis

The evaluation team applied each AVA CEM work unit. The evaluation team searched the National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search) and several other public vulnerability repositories. Searches were performed on 10 May 2022 and repeated again on 1 September 2022.

The keyword searches included the following terms:

- BL300-B2
- BL300-C2
- BL400-A1

- NXP T4240r2 QorIQ
- Power Architecture
- BLKSI.2.2.1-FIPS
- Cryptographic Support Library (CSL) Direct
- Green Hills

The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

Additionally, the evaluators performed fuzz testing of the TOE as specified in Section A.1.4 of [cPPND-SD]. The evaluators observed the TOE did not react adversely to the packets directed at the TOE or respond to the packets. This testing did not discover any vulnerabilities in the TOE.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in *Evaluation Activities for Network Device cPP*, Version 2.2e, 23 March 2020, in conjunction with Version 3.1, Revision 5 of the CC and CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the PP, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Final ETR, which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 2: Evaluated Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the guidance documentation listed in Section 6. No versions of the TOE and software, either earlier or later were evaluated.

Section 1.2 of the guidance documentation ([6]) describes the configurations necessary to comply with Commercial Solutions for Classified (CSfC) Selections for Transport Layer Security (TLS) Protected Servers and how to configure the TOE to enable CSfC compliance.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is the *Guardtime Federal Black Lantern® BL300 Series and BL400 with BLKSI.2.2.1-FIPS Security Target*, Version 1.0, 1 September 2022.

13 Abbreviations and Acronyms

AAR	Assurance Activities Report
API	Application Programming Interface
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
CSfC	Commercial Solutions for Classified
CSL	Cryptographic Support Library
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HTTPS	Hyper Text Transport Protocol-Secure
IT	Information Technology
KSI	Keyless Signature Infrastructure
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol—a means of synchronizing clocks over a computer network
NVLAP	National Voluntary Laboratory Assessment Program
PCL	Product Compliant List
POST	Power On Self-Test
PP	Protection Profile
REST	Representational State Transfer
SCI	Serial Console Interface
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. Part 1: Introduction and general model.

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. Part 2: Security functional components.

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017. Part 3: Security assurance components.

[4] Common Methodology for Information Technology Security Evaluation, Version 3.1, 5, April 2017. Evaluation methodology.

[5] collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020.

[6] Evaluation Activities for Network Device cPP, Version 2.2, December 2019.

[7] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[8] Guardtime Federal Black Lantern® BL300 Series and BL400 with BLKSI.2.2.1-FIPS Security Target, Version 1.0, 1 September 2022.

[9] Evaluation Technical Report For Guardtime Federal Black Lantern BL300 Series and BL400 with BLKSI.2.2.1-FIPS (Proprietary) Version 1.0, 1 September 2022.

[10] Assurance Activities Report for Guardtime Federal Black Lantern BL300 Series and BL400 with BLKSI.2.2.1-FIPS, Version 1.0, 1 September 2022.

[11] Guardtime Federal Black Lantern® BL300 Series and BL400 with BLKSI.2.2.1-FIPS Common Criteria Test Report and Procedures For Network Device collaborative PP, Version 2.2e, Version 1.1, Date 30 August 2022.

[11] Guardtime Federal Black Lantern Guidance Documentation, Version 1.1, September 1, 2022.