National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Guardtime Black Lantern

Report Number: CCEVS-VR-VID10838-2017
Dated: 7 December 2017
Version: 1.0

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Acknowledgements

Validation Team

Jean Petty
The Mitre Corporation

Sheldon Durrant
The Mitre Corporation

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

List of Figures

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 in 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 evaluated and tested 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 9, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Guardtime Black Lantern v1.5.2 (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 as documented in the ST.

The evaluation of Guardtime Black Lantern v1.5.2 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in December 2017. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 ([1], [2], [3], [4]) and activities specified in *Evaluation Activities for Network Device cPP*, Version 1.0, February 2015 ([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).

Guardtime Black Lantern is a network device providing an integrated hardware and software platform designed to mitigate both remote and physical attacks against a customer infrastructure and applications. Black Lantern incorporates a built-in Keyless Signature Infrastructure (KSI) gateway and extender, which implements a KSI-based data assurance and cybersecurity solution with built-in active anti-tamper measures. KSI is a method and a globally distributed network infrastructure for the issuance and verification of KSI signatures. KSI uses hash function cryptography, allowing verification to rely only on the security of hash functions and the availability of a public ledger commonly referred to as a blockchain. The blockchain is a distributed public ledger—an append-only record of events where each new event is cryptographically linked to all previous events. A user interacts with the KSI system by submitting a hash value of the data to be signed into the KSI infrastructure and is then returned a signature which provides cryptographic proof of the time of signature, integrity of the signed data, and attribution of origin. The focus of this evaluation is on the TOE functionality supporting the claims in *collaborative Protection Profile for Network Devices*, Version 1.0, 27 February 2015 ([5]). The security functionality specified in the Protection Profile includes protection of communications between the TOE and external IT entities, identification and authentication of administrators, auditing of security-relevant events, and ability to verify the source and integrity of updates to the TOE.

The Leidos evaluation team determined that the Guardtime Black Lantern v1.5.2 is conformant to the claimed Protection Profile and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) ([10]) and the 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 the ST. The evaluation also showed that the TOE is conformant to *collaborative Protection Profile for Network Devices*, v1.0, 27

February 2015, 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 are consistent with the evidence produced.

1.1 Interpretations

The following NIAP Technical Decisions were applied during the course of this evaluation:

- TD0228: NIT Technical Decision for CA certificates - basicConstraints validation
- TD0226: NIT Technical Decision for TLS Encryption Algorithms
- TD0201: NIT Technical Decision for Use of intermediate CA certificates and certificate hierarchy depth
- TD0199: NIT Technical Decision for Elliptic Curves for Signatures
- TD0188: NIT Technical Decision for Optional use of X.509 certificates for digital signatures
- TD0187: NIT Technical Decision for Clarifying FIA_X509_EXT.1 test 1
- TD0168: NIT Technical Decision for Mandatory requirement for CSR generation
- TD0156: NIT Technical Decision for SSL/TLS Version Testing in the NDcPP v1.0 and FW cPP v1.0
- TD0155: NIT Technical Decision for TLSS tests using ECDHE in the NDcPP v1.0
- TD0154: NIT Technical Decision for Versions of TOE Software in the NDcPP v1.0 and FW cPP v1.0
- TD0153: NIT Technical Decision for Auditing of NTP Time Changes in the NDcPP v1.0 and FW cPP v1.0
- TD0152: NIT Technical Decision for Reference identifiers for TLS in the NDcPP v1.0 and FW cPP v1.0
- TD0151: NIT Technical Decision for FCS_TLSS_EXT Testing - Issue 1 in NDcPP v1.0
- TD0130: NIT Technical Decision for Requirements for Destruction of Cryptographic Keys
- TD0125: NIT Technical Decision for Checking validity of peer certificates for HTTPS servers
- TD0117: NIT Technical Decision for FIA_X509_EXT.1.1 Requirement in NDcPP
- TD0116: NIT Technical Decision for a Typo in reference to RSASSA PKCS1v1_5 in NDcPP and FWcPP
- TD0112: NIT Technical Decision for TLS testing in the NDcPP v1.0 and FW cPP v1.0
- TD0111: NIT Technical Decision for third party libraries and FCS_CKM.1 in NDcPP and FWcPP
- TD0095: NIT Technical Interpretations regarding audit, random bit generation, and entropy in NDcPP
- TD0090: NIT Technical Decision for FMT_SMF.1.1 Requirement in NDcPP.

1.2 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
- Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
- Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man in the middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
- Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
- Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
- Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
- Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
- Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.

- A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.

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).

The following table provides information needed to completely identify the product and its evaluation.

Table 1: Evaluation Details

Evaluated Product:	Guardtime Black Lantern v1.5.2
Sponsor & Developer:	Guardtime 5151 California Ave. Irvine, CA 92617
CCTL:	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	December 2017
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
CEM:	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
Protection Profiles:	collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015
Disclaimer:	The information contained in this Validation Report is not an endorsement either expressed or implied of the Guardtime Black Lantern v1.5.2.
Evaluation Personnel:	Anthony Apted Greg Beaver Cody Cummins Heather Hazelhoff
Validation Personnel:	Sheldon Durrant: Lead Validator Jean Petty: Senior Validator

3 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

3.1 Security Audit

The TOE generates audit records of security relevant events. Generated audit records include the date and time of the event, the event type, the subject identity and the outcome of the event. For audit events resulting from the actions of identified users, the identity of the user is recorded in the generated audit record.

The TOE is able to store generated audit records locally and to export audit records securely to an external syslog server over TLS. In the event the space available for storing audit records locally is exhausted, the TOE will drop new audit data until such time as space is again available. The TOE keeps track of the number of dropped audit records and writes this number to the audit trail once it has been cleared and space has been made available for storage of new audit records.

The TOE writes a warning to the audit trail when the space available for storage of audit records reaches the following thresholds: 25% space remaining; 15% space remaining; 10% space remaining; 5, 4, 3, 2, and 1% space remaining.

3.2 Cryptographic Support

The TOE incorporates the Guardtime Crypto Support Library (CSL) Direct v1.0.0 to provide cryptographic algorithms and support cryptographic protocols, including TLS and HTTPS. The TOE's implementations of each of the required cryptographic algorithms is certified via the NIST Cryptographic Algorithm Validation Program (CAVP).

3.3 Identification and Authentication

The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers both a locally connected console and a network accessible interface over HTTPS (the RESTful API) to support administration of the TOE.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords. When a user is authenticated at the local console, 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 supports the use of X.509v3 certificates for TLS authentication and also supports certificate revocation checking using Online Certificate Status Protocol (OCSP). It will not accept a certificate if it is unable to establish a connection in order to determine the certificate's validity.

3.4 Security Management

The TOE implements a role-based access control model with the following three defined roles:

- Security Administrator—has authorizations to manage users (add user, update user, add user to group, delete user from group), provision Black Lantern, update TOE software, and upload certificates.

- Network Administrator—has authorizations to manage network-related configuration (device network configuration, remote host configuration).
- KSI Administrator—has authorizations to manage all KSI-related configuration (all aggregator and extender configuration).

Of these roles, only the Security and Network Administrator has the necessary authorizations to be able to manage the TOE security functionality and TSF data. Security management commands are limited to administrators and are available only after they have provided acceptable user identification and authentication data to the TOE.

3.5 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. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

The TOE provides mechanisms to view the current version of the TOE and to install updates of the TOE software. TOE updates are initiated manually by the Security Administrator. The TOE can verify the integrity of the update prior to installation using a decryption mechanism and a digital signature.

The TOE performs tests for connection integrity and cryptographic known-answer tests.

3.6 TOE Access

The TOE will terminate local interactive sessions at the local console interface after a configurable period of inactivity. 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. The remote session is terminated immediately after the request is submitted to the interface and is never open for any measurable period of inactivity.

The TOE is able to display an administrator-configurable advisory and consent warning message at the local console prior to an administrator establishing an interactive session with the TOE. The TOE provides the capability for users to terminate their own local sessions by logging out of the TOE.

3.7 Trusted Path/Channels

The TOE utilizes TLS version 1.2, in compliance with RFC 5246, to support secure path and channel communications. The TOE supports the establishment of a trusted path between a RESTful API client and the TOE, and initiated by the client. The TOE establishes trusted channels between itself and the audit server and authentication server. All TLS connections are mutual authenticated. Note that the communication with the RESTful API client and the authentication server uses HTTPS.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The ST identifies the following assumptions about the use of the product:

- The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
- The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing. For example, the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
- A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g, firewall).
- The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.
- The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.

4.2 Clarification of Scope

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* and performed by the evaluation team).
- This evaluation covers only the specific device model and 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 *Guardtime Black Lantern Security Target*, Version 1.2, 5 December 2017. 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 software and hardware and do not rely on the operational environment for any supporting security functionality.
- The TOE can be configured to use the following components in its operational environment:
    - Directly connected administrative workstation—local administration of the TOE is performed via the RS-232 serial interface
    - Remote administrative client—client software that makes requests with calls to the TOE's RESTful application programming interface (API)
    - syslog server
    - NTP server
    - authentication server
    - HTTP server, for the purpose of updating the software in the Black Lantern.
- The TOE must be installed, configured and managed as described in *Guardtime Black Lantern Guidance Documentation*, Version 1.2, December 5, 2017.

5 Architectural Information

The evaluated version of the TOE consists of the following platforms running version 1.5.2 software:

- BL300-B2
- BL300-C2

Guardtime Black Lantern is a network device providing an integrated hardware and software platform designed to mitigate both remote and physical attacks against a customer infrastructure and applications. Black Lantern incorporates a built-in Keyless Signature Infrastructure (KSI) gateway and extender, which allows for secure implementation of KSI-based data assurance and cybersecurity solutions with built-in active anti-tamper measures.

Black Lantern extends the power of the KSI Industrial Blockchain for real-time cybersecurity and data-centric asset protection, supporting enhanced continuity of operations and data loss prevention. KSI is designed to provide scalable digital signature-based authentication for electronic data, machines and humans.

KSI is a method and a globally distributed network infrastructure for the issuance and verification of KSI signatures. Unlike traditional digital signature approaches (such as Public Key Infrastructure (PKI)), which depend on asymmetric key cryptography, KSI uses only hash function cryptography, allowing verification to rely only on the security of hash functions and the availability of a public ledger commonly referred to as a blockchain.

A blockchain is a distributed public ledger—an append-only record of events where each new event is cryptographically linked to the previous. New entries are created using a distributed consensus protocol.

The KSI blockchain overcomes three major weaknesses of mainstream blockchain technologies—which were designed to facilitate asset transactions—making KSI suitable also for cybersecurity and data governance applications:

- Scalability—one of the most significant challenges with traditional blockchain approaches is scalability – they scale at O(n) complexity, meaning they grow linearly with the number of transactions. In contrast the KSI blockchain scales at O(t) complexity – it grows linearly with time and independently from the number of transactions. KSI can sustain billions of asset registration events every second without growing out of control.
- Settlement time—in contrast to the widely distributed crypto-currency approach, the number of participants in KSI blockchain distributed consensus protocol is limited. By limiting the number of participants, it becomes possible to achieve consensus synchronously, eliminating the need for Proof of Work and ensuring settlement can occur within one second.
- Formal security proof—unlike other blockchains, KSI blockchain has been subjected to end-to-end formal mathematical proof that provides assurance that the protocol does precisely what it says it does.

A user interacts with the KSI system by submitting a hash value of the data to be signed into the KSI infrastructure and is then returned a signature which provides cryptographic proof of the time of signature, integrity of the signed data, as well as attribution of origin, i.e., which entity generated the signature.

Figure 1 depicts a sample topology for the Guardtime Black Lantern TOE.

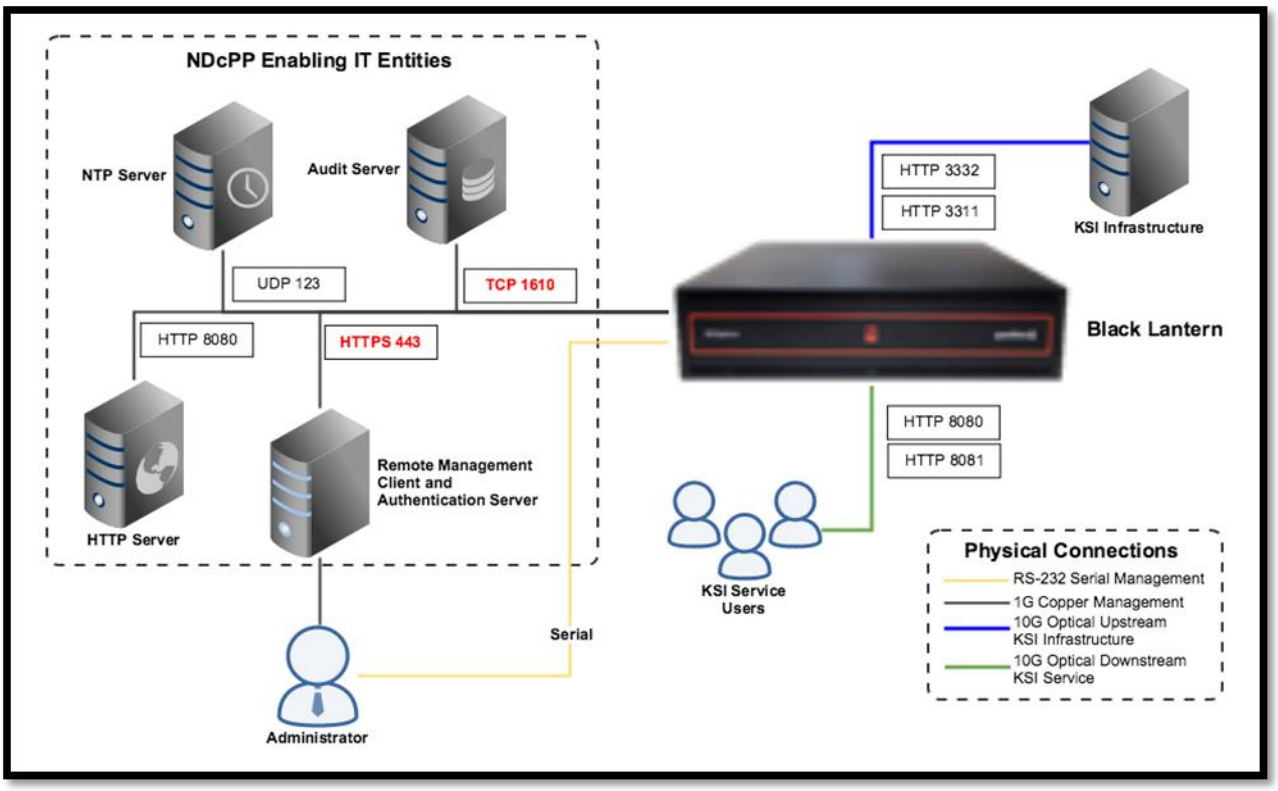

Figure 1: Sample Guardtime Black Lantern Network Topology

6 Documentation

Guardtime provides *Guardtime Black Lantern Guidance Documentation*, Version 1.2, December 9, 2017 for the end users of the TOE, providing guidance on the installation, configuration and use of the TOE. This document was specifically examined in the context of the evaluation.

7 Independent Testing

This section summarizes evaluation team testing of the TOE. It is based on information contained in *Guardtime Black Lantern Common Criteria Test Report and Procedures*, Version 1.1, 6 December 2017 ([11]).

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to the *collaborative Protection Profile for Network Devices*, Version 1.0, 27 February 2015.

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *Evaluation Activities for Network Device cPP*, Version 1.0, February 2015. The Test Plan describes how each test activity was 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 listed above.

Independent testing of the TOE initially took place from May 29, 2017 to June 2, 2017 onsite at Guardtime in Irvine, CA. Testing continued periodically between June 26, 2017 and September 18, 2017 at the Leidos CCTL facility in Columbia, Maryland.

7.1 Test Configuration

Evaluation team testing used the TOE configuration depicted in Figure 2.

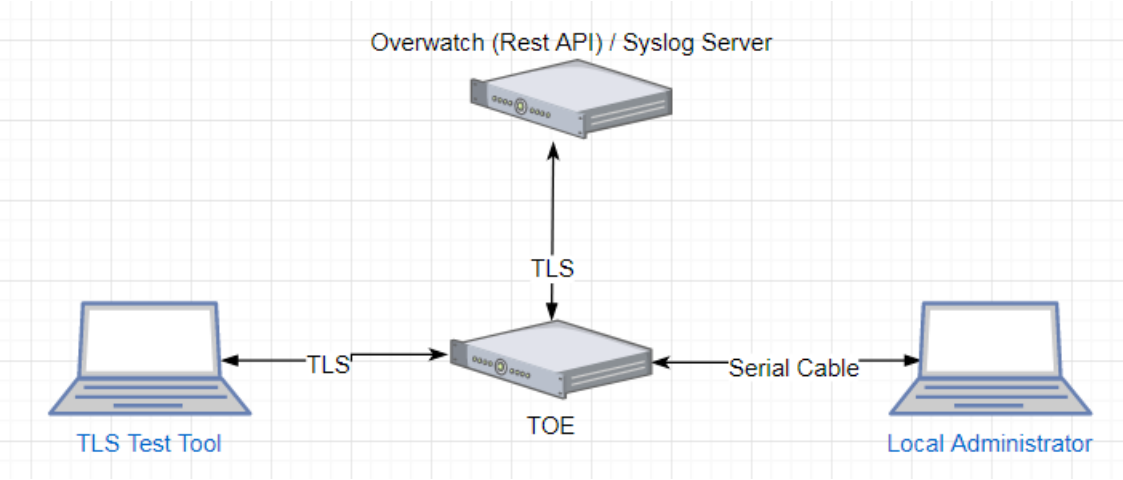

Figure 2: Test Configuration

The following hardware and software components were included in the evaluated configuration during testing:

- Hardware:
  - BL300-B2 appliance
- Software:
  - Black Lantern v1.5.2.

The following components are not part of the TOE but were included in the testing environment:

- Local administration laptop—directly connected to RS-232 console port
- RESTful API client—Overwatch (a Guardtime-developed server framework that can be used as a remote administration client for Black Lantern)

- Remote authentication server—for testing purposes, co-located on the same server as the Overwatch client
- Audit server—Rsyslog v8.27
- NTP server
- TLS test tool—used to assist in testing TOE's implementation of TLS protocol.

The evaluation team followed the installation and configuration procedures documented in the product guidance to install the TOE in the test environment.

Subsequently, the evaluators exercised all the test cases. The tests were selected in order to ensure that each of the test assertions specified in *Evaluation Activities for Network Device cPP* were covered. All tests passed. A summary of the testing performed by the evaluation team is provided in *Guardtime Black Lantern Common Criteria Assurance Activities Report*.

7.2 Vulnerability Analysis

The evaluation team performed a vulnerability analysis following the processes described in the CEM and using the flaw-hypothesis methodology. This included a search of public vulnerability databases and development of Type 3 flaw hypotheses in accordance with Section A.3 of [6]. 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.

8 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in *Evaluation Activities for Network Device cPP*, Version 1.0, February 2015, in conjunction with Version 3.1, Revision 4 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 claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 2: TOE Security 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

9 Validator Comments/Recommendations

None

10 Annexes

Not applicable

11 Security Target

The ST for this product's evaluation is *Guardtime Black Lantern Security Target*, Version 1.2, December 5, 2017.

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

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
CM	Configuration Management
ETR	Evaluation Technical Report
HTTP(S)	Hypertext Transfer Protocol (Secure)
IT	Information Technology
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
PP	Protection Profile
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report

13 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.

[5] collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015.

[6] Evaluation Activities for Network Device cPP, Version 1.0, February 2015.

[7] Guardtime Black Lantern Security Target, Version 1.2, December 5, 2017.

[8] Guardtime Black Lantern Guidance Documentation, Version 1.2, December 5, 2017.

[9] Evaluation Technical Report for Guardtime Black Lantern, Part 2 (Leidos Proprietary), Version 1.0, 7 December 2017.

[10] Guardtime Black Lantern Common Criteria Assurance Activities Report, Version 1.0, 7 December 2017.

[11] Guardtime Black Lantern Common Criteria Test Report and Procedures, Version 1.1, 6 December 2017.