National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

TM

Validation Report
for the
Cigent PBA Software v1.0.6

Report Number: CCEVS-VR-VID11378-2023
Dated: October 24, 2023
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

Jerome Myers

The Aerospace Corporation

Farid Ahmed

Anne Gugel

Richard Toren

Robert Wojcik

Johns Hopkins University – Applied Physics Laboratory

Common Criteria Testing Laboratory

Kevin Steiner

Lightship Security USA, Inc.

Table of Contents

1. Executive Summary 1
2. Identification 2
3. Architectural Information 4
    3.1. TOE Evaluated Configuration 4
    3.2. Physical Boundary 4
    3.3. Required Non-TOE Hardware, Software, and Firmware 4
4. Security Policy 5
    4.1. Data Protection 5
    4.2. Secure Key Material 5
    4.3. Secure Managment 5
    4.4. Trusted Update 5
    4.5. Cryptographic Operations 5
5. Assumptions 6
6. Clarification of Scope 8
7. Documentation 9
8. IT Product Testing 10
    8.1. Developer Testing 10
    8.2. Evaluation Team Independent Testing 10
    8.3. Evaluated Configuration 10
9. Results of the Evaluation 12
    9.1. Evaluation of Security Target (ASE) 12
    9.2. Evaluation of Development Documentation (ADV) 12
    9.3. Evaluation of Guidance Documents (AGD) 12
    9.4. Evaluation of Life Cycle Support Activities (ALC) 13
    9.5. Evaluation of Test Documentation and the Test Activity (ATE) 13
    9.6. Vulnerability Assessment Activity (VAN) 13
    9.7. Summary of Evaluation Results 14
10. Validator Comments 15
11. Annexes 16
12. Security Target 17
13. Glossary 18

14. Acronym List 19
15. Bibliography 20

List of Tables

Table 1: Evaluation Identifiers..... 2
Table 3: Assumptions 6
Table 4: Tools Used for Testing 11

1. Executive Summary

This Validation Report (VR) report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cigent PBA Software v1.0.6 provided by Cigent. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

This VR 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. In conjunction with this VR, end-users should review the Security Target[6] (ST), which is where specific security claims are made. The ST also describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in October 2023. The information in this report is largely derived from the Evaluation Technical Report[11] (ETR) and associated test reports, all written by Lightship Security (LS). The evaluation determined that the product is both Common Criteria Part 2[1] Extended and Part 3[2] Conformant and meets the assurance requirements of the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, v2.0 + Errata 20190201[4].

The TOE is Cigent PBA Software v1.0.6. The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5)[3] for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR[11]. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target[6] (ST). The conclusions of the testing laboratory in the ETR[11] are consistent with the evidence produced. Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Lightship evaluation team determined that the TOE is conformant to the claimed Protection Profile[4], and when installed, configured and operated as described in the evaluated guidance documentation, satisfies all the SFRs specified in the ST[6].

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, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM[3]) 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 information technology 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 Validated Products List.

Table 1 provides information needed to completely identify the product, to include:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Cigent PBA Software v1.0.6
Sponsor and Developer	Cigent 2211 Widman Way, Suite 150 Fort Myers, Florida 33901
CCTL	Lightship Security USA, Inc. 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	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.

Item	Identifier
Protection Profile	collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, v2.0 + Errata 20190201
Security Target	Cigent PBA Software v1.0.6 Security Target, v2.5
Evaluation Technical Report	Cigent PBA Software v1.0.6 Evaluation Technical Report, v0.8
Conformance Result	CC Part 2[1] extended, CC Part 3[2] conformant
Evaluation Personnel	Kevin Steiner
CCEVS Validators	Jerome Myers, Farid Ahmed, Anne Gugel, Richard Toren, Robert Wojcik

3. Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1. TOE Evaluated Configuration

The TOE is software that provides pre-boot authentication (PBA) for use with a self-encrypting drive (SED). TOE Evaluated Configuration The TOE is Cigent PBA Software v1.0.6 software that provides pre-boot authentication (PBA) for use with a self-encrypting drive (SED). The evaluated configuration consists of Cigent PBA Software v1.0.6 configured in accordance with the documentation listed in Section 7 of this VR. The TOE must be installed, configured and managed as described in the documentation referenced in Section 7.

3.2. Physical Boundary

The physical boundary of the TOE encompasses the Cigent PBA Software v1.0.6. The TOE runs on Ubuntu 22.04 and is provided and installed as a single software package. Users may download the software after purchase from Cigent's web portal (https://download.cigent.com/Cigent_PBA_v1.0.6.zip). Alternatively, the TOE may come preinstalled on a partner original equipment manufacturer (OEM) Opal2 compatible solid state drive (SSD).

3.3. Required Non-TOE Hardware, Software, and Firmware

The TOE operates with the following components in the environment:

- **SED.** Opal 2.0 compliant SED.
- **Protected OS.** The TOE supports protection of Windows 10 based Operating Systems.
- **Computer Hardware.** Intel based unified extensible firmware interface (UEFI) booted systems that supports Intel Secure Key Technology. Note: CC testing performed using the following central processing unit (CPU): Intel Core i7-8550U.
- **Smartcard and reader.** When dual factor authentication is used, FIPS 201 Personal Identity Verification Common Access Card (PIV-CAC) compliant smartcards and readers are required.

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1. Data Protection

The TOE enables encryption of data on a storage device to protect it from unauthorized disclosure. The TOE enables the data encryption function of a SED drive by providing pre-boot user authentication and key management capabilities.

4.2. Secure Key Material

The TOE ensures key material used for storage encryption is properly generated and protected from disclosure. It also implements cryptographic key and key material destruction during transitioning to a Compliant power saving state, or when all keys and key material are no longer needed.

4.3. Secure Management

The TOE enables management of its security functions.

4.4. Trusted Update

The TOE ensures the authenticity and integrity of software updates through digital signatures using Rivest Shamir Adleman (RSA) 4096 with Secure Hash Algorithm (SHA) SHA-512.

4.5. Cryptographic Operations

The TOE implements a cryptographic module. The cryptographic module uses CAVP validated cryptographic algorithms.

5. Assumptions

Table 2: Assumptions

Identifier	Description
A.INITIAL_DRIVE_STATE	Users enable Full Drive Encryption on a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption. The cPP does not intend to include requirements to find all the areas on storage devices that potentially contain protected data. In some cases, it may not be possible – for example, data contained in "bad" sectors. While inadvertent exposure to data contained in bad sectors or un-partitioned space is unlikely, one may use forensics tools to recover data from such areas of the storage device. Consequently, the cPP assumes bad sectors, un-partitioned space, and areas that must contain unencrypted code (e.g., MBR and AA/EE pre-authentication software) contain no protected data.
A.SECURE_STATE	Upon the completion of proper provisioning, the drive is only assumed secure when in a powered off state up until it is powered on and receives initial authorization.
A.TRUSTED_CHANNEL	Communication among and between product components (e.g., AA and EE) is sufficiently protected to prevent information disclosure. In cases in which a single product fulfils both cPPs, then the communication between the components does not extend beyond the boundary of the TOE (e.g., communication path is within the TOE boundary). In cases in which independent products satisfy the requirements of the AA and EE, the physically close proximity of the two products during their operation means that the threat agent has very little opportunity to interpose itself in the channel between the two without the user noticing and taking appropriate actions.
A.TRAINED_USER	Authorized users follow all provided user guidance, including keeping password/passphrases and external tokens securely stored separately from the storage device and/or platform.
A.PLATFORM_STATE	The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product.

Identifier	Description
A.SINGLE_USE_ET	External tokens that contain authorization factors are used for no other purpose than to store the external token authorization factors.
A.POWER_DOWN	The user does not leave the platform and/or storage device unattended until all volatile memory is cleared after a power-off, so memory remnant attacks are infeasible. Authorized users do not leave the platform and/or storage device in a mode where sensitive information persists in non-volatile storage (e.g., lock screen). Users power the platform and/or storage device down or place it into a power managed state, such as a "hibernation mode".
A.PASSWORD_STRENGTH	Authorized administrators ensure password/passphrase authorization factors have sufficient strength and entropy to reflect the sensitivity of the data being protected.
A.PLATFORM_I&A	The product does not interfere with or change the normal platform identification and authentication functionality such as the operating system login. It may provide authorization factors to the operating system's login interface, but it will not change or degrade the functionality of the actual interface.
A.STRONG_CRYPTO	All cryptography implemented in the Operational Environment and used by the product meets the requirements listed in the cPP. This includes generation of external token authorization factors by a RBG.
A.PHYSICAL	The platform 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 platform's correct operation.

6. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_FDE_AA_V2.0E[4] 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 in accordance with the evaluation activities specified in CPP_FDE_AA_V2.0E-SD[5] 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.
- 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[6]. The CEM[3] defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

  The functionality evaluated is scoped exclusively to the Cigent PBA Software v1.0.6 Security Target, v2.5[6] and security functional requirements specified in the CPP_FDE_AA_V2.0E[4] and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *Cigent PBA Software v1.0.6 Common Criteria Guide*, v1.2[7]
- *Cigent PBA Installation Guide and User Manual*, Aug 2023, V21[8]

All documentation delivered with the product is relevant to and within the scope of the TOE. To use the product in the evaluated configuration, the product must be configured as specified in this documentation.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

8. IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *Cigent PBA Software v1.0.6 Assurance Activity Report, v0.12*[9] provides an overview of testing and the prescribed evaluation activities.

8.1. Developer Testing

No evidence of developer testing is required in the SARs or Evaluation Activities.

8.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing at Lightship Security USA in Baltimore, MD from March 2023 until August 2023. Follow-up testing was conducted from October 2, 2023 to October 4, 2023 and October 12, 2023 to address validation comments. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target[6].

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST[6].

The Evaluation team used the Protection Profile[4] test procedures as a basis for creating each of the independent tests as required by the Evaluation Activities.

Each Evaluation Activity was tested as required by the conformant Protection Profile[4] and the evaluation team verified that each test passed.

8.3. Evaluated Configuration

The TOE is the Cigent PBA Software v1.0.6. The TOE testing environment components are identified in Figure 1 and Table 3 below.

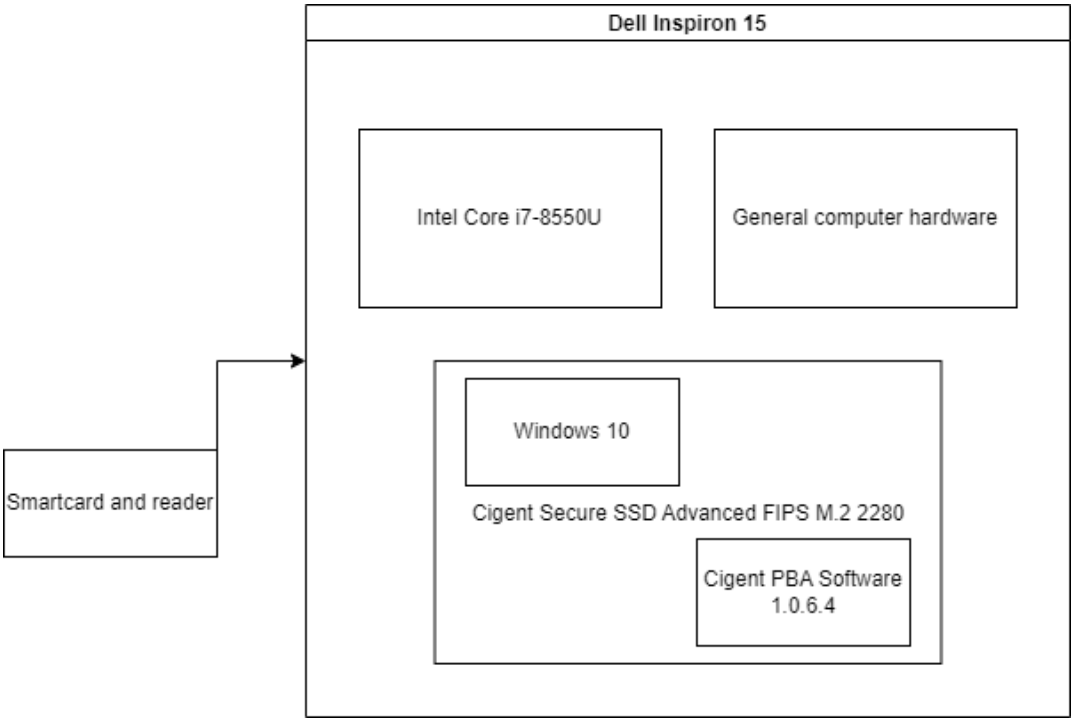

Figure 1: Testing Environment Overview

Table 3: Tools Used for Testing

Tool name	Version	Description
Cigent PBA Software 1.0.6.4 MEMTEST	1.0.6.4 MEMTEST	Instrumented TOE build to allow the evaluator to capture key values and offsets then dump memory to verify key destruction. This tool was used for FCS_CKM.4(d) testing only.
HxD	2.5.0.0	This tool was used to verify binary file dumps with key contents

9. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR)[12, 13] and the Evaluation Technical Report (ETR)[11]. The reader of this document can assume that all activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC Version 3.1 Revision 5 and CEM[3] Version 3.1 Revision 5. The evaluation determined Cigent PBA Software v1.0.6 to be Part 2[1] extended conformant, and meets the SARs contained in the PP[4]. Additionally, the evaluator performed the Evaluation Activities specified in CPP_FDE_AA_V2.0E-SD[5].

The evaluation determined the TOE satisfies the conformance claims made in the Cigent PBA Software v1.0.6 Security Target, of Part 2[1] extended and Part 3[2] extended. The TOE satisfies the requirements specified in the PP[4] listed above.

9.1. Evaluation of Security Target (ASE)

The Evaluation team applied each ASE CEM[3] work unit. The ST[6] evaluation ensured the ST[6] contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cigent PBA Software v1.0.6 that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM[3], and that the conclusion reached by the Evaluation team was justified.

9.2. Evaluation of Development Documentation (ADV)

The Evaluation team applied each ADV CEM[3] work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed PP[4] for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST[6] and product guidance documentation providing descriptions of the TOE external interfaces.

The Validation reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM[3], and that the conclusion reached by the Evaluation team was justified.

9.3. Evaluation of Guidance Documents (AGD)

The Evaluation team applied each AGD CEM[3] work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in

describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM[3], and that the conclusion reached by the Evaluation team was justified.

9.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM[3] work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM[3], and that the conclusion reached by the Evaluation team was justified.

9.5. Evaluation of Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM[3] work unit. The Evaluation team ran the set of tests specified by the Test Evaluation Activities and recorded the results in a Test Report[12, 13], summarized in the AAR[9].

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM[3], and that the conclusion reached by the Evaluation team was justified.

9.6. Vulnerability Assessment Activity (VAN)

The evaluation team performed each AVA evaluation activity and applied each AVA CEM[3] work unit. The vulnerability analysis is in the Cigent PBA Software v1.0.6 Vulnerability Assessment, Version 0.3[10], report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities was last conducted on October 2, 2023, did not uncover any residual vulnerability. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. This comprised a search of public vulnerability databases.

The Evaluation team searched:

- Common Vulnerabilities and Exposures
    - NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search

    - Common Vulnerabilities and Exposures: https://cve.mitre.org/cve/search_cve_list.html
- US-CERT: http://www.kb.cert.org/vuls/html/search

The Evaluation team performed a search using the following keywords:

- Cigent
- Cigent PBA Software v1.0.6.4
- Drive encryption
- Disk encryption
- Key destruction
- Key sanitization
- Self Encrypting Drive (SED)
- OPAL
- Key Caching
- Opal management software
- SED management software
- Openssl 3.0.7
- Sqlcipher 4.5.1
- Zlib 1.2.12
- Gzip 0.1.0
- Libpcsclite1 1.9.5-3

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM[3], and that the conclusion reached by the Evaluation team was justified.

9.7. Summary of Evaluation Results

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST[6] are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST[6].

The Validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM[3] and performed the Evaluation Activities in CPP_FDE_AA_V2.0E-SD[5], and correctly verified that the product meets the claims in the ST[6].

10. Validator Comments

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 7 of this Validation Report to ensure the evaluated configuration is established and maintained. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST[6]. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. No versions of the TOE and software, either earlier or later, were evaluated.

11. Annexes

Not applicable.

12. Security Target

Cigent PBA Software v1.0.6 Security Target, v2.5, 10 October 2023.

13. GLOSSARY

- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance:** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature:** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

15. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002*, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003*, Version 3.1 Revision 5, April 2017
3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
4. *Collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition* Version 2.0 + Errata 20190201
5. *Supporting Document Mandatory Technical Document Full Drive Encryption: Authorization Acquisition* February 2019 Version 2.0 + Errata 20190201
6. *Cigent PBA Software v1.0.6 Security Target*, v2.5
7. *Cigent PBA Software v1.0.6 Common Criteria Guide*, v1.2
8. *Cigent PBA Installation Guide and User Manual*, Aug 2023, V21
9. *Cigent PBA Software v1.0.6 Assurance Activity Report*, v0.12
10. *Cigent PBA Software v1.0.6 Vulnerability Assessment*, Version 0.3
11. *Cigent PBA Software v1.0.6 Evaluation Technical Report*, v0.8
12. *Cigent PBA Software v1.0.6 cPP_FDE_AA Test Plan*, Version 0.5
13. *Cigent PBA Software v1.0.6 cPP_FDE_AA Test Plan Evidence*, Version 0.5