Cigent PBA Software v1.0.6

Common Criteria Guide

Version 1.2

September 2023

Document prepared by

www.lightshipsec.com

Table of Contents

List of Tables

1 About this Guide

1.1 Overview

1 This guide provides supplemental instructions and related information to achieve the Common Criteria evaluated configuration of Cigent PBA Software v1.0.6.

1.2 Audience

2 This guide is intended for system administrators and the various stakeholders involved in the Common Criteria evaluation. It is assumed that readers will use this guide in conjunction with the related documents listed in Table 2.

1.3 About the Common Criteria Evaluation

3 The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) is an international standard for security certification of IT products and systems. More information is available at https://www.commoncriteriaportal.org/

1.3.1 Protection Profile Conformance

4 The Common Criteria evaluation was performed against the requirements of the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, v2.0 + Errata 20190201, available at https://www.niap-ccevs.org/Profile/PP.cfm

1.3.2 Evaluated Software

5 The Target of Evaluation (TOE) is the Cigent PBA Software v1.0.6 software.

6 Users may download the software after purchase from Cigent's secure web portal. Alternatively, the TOE may come preinstalled on a partner OEM Opal2 compatible SSD disk.

7 Users may verify that they have the correct version of the TOE, after login, by referencing the version displayed in the Summary section of the Dashboard.

1.3.3 Non-TOE Components

8 The TOE operates with the following components in the environment:

a) **SED**. Opal 2.0 compliant SED. CC testing performed using the following:

- Cigent Secure SSD Advanced FIPS M.2 2280

b) **Protected OS.** The TOE supports protection of Windows 10 based Operating Systems. CC testing performed using OS's:

- Microsoft Windows 10

c) **Computer Hardware.** Intel based UEFI booted systems that supports Intel Secure Key Technology. CC testing performed using the following CPUs:

- Intel Core i7-8550U

d) **Smartcard and reader**. When smartcard only or dual factor authentication is used, FIPS 201 Personal Identity Verification Common Access Card (PIV-CAC) compliant smartcards and readers are required.

1.3.4 Evaluated Functions

9 The following functions have been evaluated under Common Criteria:

a) **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.

b) **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.

c) **Secure Management.** The TOE enables management of its security functions, including:

- forwarding requests to change the Data Encryption Key (DEK) to the SED,
- forwarding requests to cryptographically erase the DEK to the SED,
- allowing authorized users to change authorization factors or set of authorization factors used,
- initiate TOE firmware/software updates.

d) **Trusted Update.** The TOE ensures the authenticity and integrity of software updates through digital signatures using RSA 4096 with SHA-512.

e) **Cryptographic Operations.** The cryptographic algorithms used in the above functions have been validated for correct implementation.

10 **NOTE:** No claims are made regarding any other security functionality.

1.3.5 Evaluation Assumptions

11 The following assumptions are defined by the Common Criteria Protection Profile. The guidance shown in the table below should be followed to uphold these assumptions in the operational environment.

Table 1: Evaluation Assumptions

Assumption	Guidance
Communication among and between product components (i.e., AA and EE) is sufficiently protected to prevent information disclosure.	In this case, Cigent PBA is the Authorization Acquisition (AA) component, and the SED is the Encryption Engine (EE) component.
The Operational Environment (OE) provides a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption.	SEDs should be formatted prior to use with Cigent PBA.
An authorized administrator will be responsible for ensuring that the passphrase authorization factor conforms to guidance from the Enterprise using the TOE.	Administrators should ensure that Cigent PBA users are aware of organizational password policies.

Assumption	Guidance
Volatile memory is cleared after power-off so memory remnant attacks are infeasible.	No action is required.
External tokens that contain authorization factors will be used for no other purpose than to store the external token authorization factor.	Cigent PBA may be used with Smart Cards. The Smart Cards should only be used for identification purposes.
The Operating Environment will provide a cryptographic function capability that is commensurate with the requirements and capabilities of the TOE and Appendix A (of the Protection Profile).	No action is required. By default, the Cigent PBA may only be configured to use the cryptographic functions provided by the underlying Operating System.
Authorized users will be properly trained and follow all guidance for securing the TOE and authorization factors.	Administrators should be familiar with this document and should ensure that users are trained in using Cigent PBA. Administrators and users must protect passwords and smartcards in accordance with organizational policies.
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.	Cigent PBA does not provide malware protection.
The Operational Environment will provide individual user identification and authentication mechanisms that operate independently of the authorization factors used by the TOE.	The protected OS that boots after SED unlock should require users to authenticate.
The Operational Environment will provide a secure physical computing space such than an adversary is not able to make modifications to the environment or to the TOE itself.	Devices protected by Cigent PBA should be physically protected in accordance with organizational policies.

1.4 Related Documents

12 This guide supplements the below documents which are available from Cigent's web portal.

Table 2: Related Documents

Reference	Document
[MAN]	Cigent PBA Installation Guide and User Manual, V21

13 **NOTE:** The information in this guide supersedes related information in other documentation.

2 Guidance

2.1 Protected OS Configuration

14 The ‘Sleep’ and ‘Hibernate’ power states should be disabled in the protected OS that boots after SED unlock. The compliant power states supported by Cigent PBA are described in section 2.5 below.

15 **NOTE:** The TOE is designed to authorize access to data secured by a SED. Customers are encouraged to review any security interactions between the underlying platform, the protected OS, and SEDs to ensure appropriate security practices to prevent access to the unlocked SED. The following practices are recommended:

a) Configure a BIOS admin password

b) Disable boot from portable media (e.g., USB)

c) Disable warm boot options such as Fast Startup

2.2 Configuration

16 Follow the instructions in [MAN] to install and configure the TOE in accordance with your requirements. There are no specific steps required to establish the evaluated configuration.

17 These instructions are the same for all operational environments.

2.3 Authorization Factors

18 Cigent PBA supports the following authorization factors:

a) **Passwords.** Users authenticate by means of a password. See [MAN] *Username and Password Requirements.*

b) **Smart Card.** Users authenticate using a PIV-CAC smart card. See [MAN] *Add User*.

c) **Multi-Factor.** Both passwords and Smart Cards are used in this case. Smart Cards must be FIPS201 PIV-CAC compliant. See [MAN] *Add User* and *Settings > Require Two-Factor Authentication*.

2.4 Cryptographic Key Destruction

19 The TOE handles the destruction of cryptographic keys and key material when they are no longer required. There are no situations where key destruction would be delayed or prevented.

20 Transitioning to the supported power saving state also triggers the destruction of any plaintext keys and key material from volatile memory.

2.5 Power Saving States

21 The TOE supports the following power saving states:

a) **G3 – Mechanical Off.** In this state, the system is completely off and it does not consume any power. The system returns to the working state only after a

complete reboot and invocation of the Cigent PBA for authentication/authorization. Successful authentication and authorization must be achieved using the authorization factors described in section 2.3 in order to resume access to protected data.

22 An unexpected power loss would result in the G3 power state. When resuming from the above power saving states, users are required to successfully re-authenticate using the same authorization factors described in section 2.3 as per normal operation.

23 Users interact with the protected OS or hardware platform to enter the above power states. Refer to the protected OS guidance for instructions on entering the above power state.

2.6 Management Functions

24 Cigent PBA provides the following management functions as relevant to the Common Criteria Protection Profile:

a) **Request change of DEK.** See [MAN] *Uninstall PBA* and *Erase Entire Disk*.

b) **Request cryptographic erase of DEK.** See [MAN] *Uninstall PBA* and *Erase Entire Disk.*

c) **User change of authorization factors.** See [MAN] *Add User* and *Edit User* and *Settings* > *Require Two-Factor Authentication*.

d) **Initiate firmware/software updates.** See section 2.7 below.

25 **Note**: Changing the DEK is the same functionality as cryptographically erasing the DEK.

2.7 Updating Cigent PBA

26 TOE updates may be performed by booting the host system with a USB drive that contains the PBA OS, utility, and the updated PBA content. An admin user must authenticate and choose to install the update.

27 Update files are digitally signed by Cigent and verified by the TOE prior to installation. Only authorized administrators may perform the update process. If signature verification is successful, the TOE boots as per normal. If signature verification fails, the update is aborted and an error message is displayed: "*Failed to load Pre-Boot. Validation failed*".

28 For specific instructions on how to update the TOE, refer to Section 6 of [MAN].

2.8 Cryptography

29 The TOE supports a 256-bit DEK using AES-GCM-256. No other configuration of cryptographic parameters is possible/required.