National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Archon Linux Unified Key Setup (LUKS) v3.0.0.2

Report Number: CCEVS-VR-VID11568-2025
Dated: May 19, 2025
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 George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Clare Parran

Lori Sarem

Chris Thorpe

The MITRE Corporation

Common Criteria Testing Laboratory

Saniya Shaikh

Yogesh Pawar

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (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 for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this 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 5 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 the Archon Linux Unified Key Setup (LUKS) Series Target of Evaluation (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 was completed by Acumen Security in May 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019 (FDE_AA) and collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 (FDE_EE).

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the Protection Profile (PP). 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 and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation Team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, 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 ETR 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, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

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.

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

- 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(s) 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	Archon Linux Unified Key Setup (LUKS) v3.0.0.2
Protection Profile	collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019 (FDE_AA) and collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 (FDE_EE)
Security Target	Archon Linux Unified Key Setup (LUKS) Security Target, Version 2.10, May 13, 2025
Evaluation Technical Report	Evaluation Technical Report for Archon Linux Unified Key Setup (LUKS) v3.0.0.2, Version 1.9, May 13, 2025
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor/Developer	CACI
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd Suite 395 Rockville, MD 20850
CCEVS Validators	Lisa Mitchell, Clare Parran, Chris Thorpe

3 Architectural Information

Archon Linux Unified Key Setup (LUKS) is a software Full Drive Encryption (FDE) product that is integrated into Archon Operating System (a Red Hat Enterprise Linux (RHEL) v8.10 derivative). It provides an FDE solution for the single hard drive installed in laptop models.

Archon LUKS is used to encrypt a block device. The contents of the encrypted device are arbitrary, and therefore any filesystem can be encrypted, including swap partitions. There is an unencrypted header at the beginning of an encrypted volume, which allows up to 32 encryption keys to be stored (in an encrypted form) along with encryption parameters such as cipher type and key size.

By default, the option to encrypt the block device is selected during the Archon OS installation. The system prompts users for a LUKS passphrase every time the system is booted. This passphrase unlocks the bulk encryption key that decrypts the data.

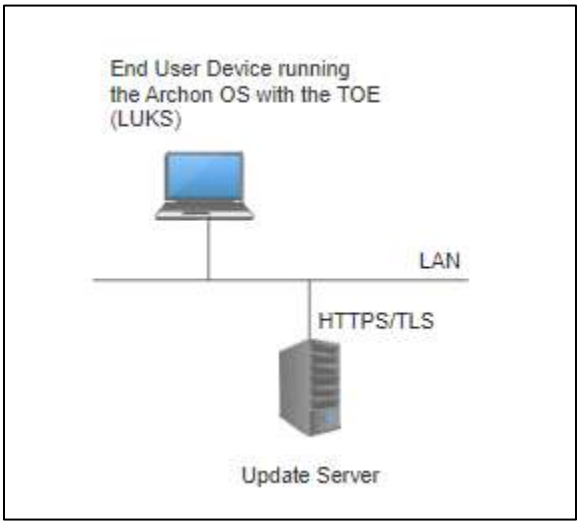
Archon LUKS provides a set of tools that simplifies managing encrypted devices. With Archon LUKS, you can encrypt block devices and enable multiple user keys to decrypt a master key.

3.1 Physical Boundary

3.1.1 TOE in the Operational Environment - Deployment

The diagram below depicts a representative TOE deployment.

Figure 1: Representative TOE Deployment



The following items are required for the operational environment.

Table 1: Hardware and Software Environmental Components

Components	Mandatory/ Optional	Description
End User Device (EUD)	Mandatory	The hardware running Archon OS with LUKS enabled (the TOE).
Update Server	Mandatory	Provides the ability to check for TOE software updates as well as providing signed updates. The communication is performed by the Operational Environment (Archon OS).

4 Security Policy

The TOE provides the security functions required by the FDE_AA cPP and FDE_EE cPP.

4.1 Cryptographic Support

The TOE includes NIST CAVP-validated cryptographic algorithms supporting cryptographic functions. The TOE provides Key Derivation, BEV (Border Encrypt Value) Validation, and data encryption.

4.2 User Data Protection

The TOE performs Full Drive Encryption such that the drive contains no plaintext user data. The TOE performs user data encryption by default in the out-of-the-box configuration using XTS-AES-256 mode.

4.3 Security Management

The TOE supports management functions for changing and erasing the DEK, modifying the passphrase, and initiating the TOE updates using a command line interface.

4.4 Protection of the TSF

The TOE provides trusted firmware updates, protects Key and Key Material; and supports power saving states. The TOE runs a suite of self-tests during initial start-up (on power on).

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 2: Assumptions

ID	Assumption
A.INITIAL_DRIVE_STATE/AA	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.INITIAL_DRIVE_STATE/EE	Users enable Full Drive Encryption on a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption. It is also assumed that data intended for protection should not be on the targeted storage media until after provisioning. 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.PASSWORD_STRENGTH/AA	Authorized administrators ensure password/passphrase authorization factors have sufficient strength and entropy to reflect the sensitivity of the data being protected.
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.

ID	Assumption
A.PLATFORM_I&A/AA	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.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.
A.POWER_DOWN/AA	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.POWER_DOWN/EE	The user does not leave the platform and/or storage device unattended until all volatile memory is cleared after a power-off. This properly clears memories and locks down the device. 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 or sleep state). Users power the platform and/or storage device down or place it into a power managed state, such as a “hibernation mode”.
A.SECURE_STATE/AA	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.SINGLE_USE_ET/AA	External tokens that contain authorization factors are used for no other purpose than to store the external token authorization factors.
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.TRAINED_USER/AA	Authorized users follow all provided user guidance, including keeping password/passphrases and external tokens securely stored separately from the storage device and/or platform.

ID	Assumption
A.TRAINED_USER/EE	Users follow the provided guidance for securing the TOE and authorization factors. This includes conformance with authorization factor strength, using external token authentication factors for no other purpose and ensuring external token authorization factors are securely stored separately from the storage device and/or platform. The user should also be trained on how to power off their system.
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.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Table 3: Threats

ID	Threat
T.AUTHORIZATION_GUESSING/AA	Threat agents may exercise host software to repeatedly guess authorization factors, such as passwords and PINs. Successful guessing of the authorization factors may cause the TOE to release BEV or otherwise put it in a state in which it discloses protected data to unauthorized users.
T.AUTHORIZATION_GUESSING/EE	Threat agents may exercise host software to repeatedly guess authorization factors, such as passwords and PINs. Successful guessing of the authorization factors may cause the TOE to release DEKs or otherwise put it in a state in which it discloses protected data to unauthorized users.
T.CHOSEN_PLAINTEXT/EE	Threat agents may trick authorized users into storing chosen plaintext on the encrypted storage device in the form of an image, document, or some other file. A poor choice of

ID	Threat
	encryption algorithms, encryption modes, and initialization vectors along with the chosen plaintext could allow attackers to recover the effective DEK, thus providing unauthorized access to the previously unknown plaintext on the storage device.
T.KEYING_MATERIAL_COMPROMISE/AA	Possession of any of the keys, authorization factors, submasks, and random numbers or any other values that contribute to the creation of keys or authorization factors could allow an unauthorized user to defeat the encryption. The cPP considers possession of key material of equal importance to the data itself. Threat agents may look for key material in unencrypted sectors of the storage device and on other peripherals in the operating environment (OE), e.g. BIOS configuration, SPI flash.
T.KEYING_MATERIAL_COMPROMISE/EE	Possession of any of the keys, authorization factors, submasks, and random numbers or any other values that contribute to the creation of keys or authorization factors could allow an unauthorized user to defeat the encryption. The cPP considers possession of keying material of equal importance to the data itself. Threat agents may look for keying material in unencrypted sectors of the storage device and on other peripherals in the operating environment (OE), e.g. BIOS configuration, SPI flash, or TPMs.
T.KEYSPACE_EXHAUST	Threat agents may perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms and/or parameters allow attackers to exhaust the key space through brute force and give them unauthorized access to the data.
T.KNOWN_PLAINTEXT/EE	Threat agents know plaintext in regions of storage devices, especially in uninitialized regions (all zeroes) as well as regions that contain well known software such as operating systems. A poor choice of encryption algorithms, encryption modes, and initialization vectors along with known plaintext could allow an attacker to recover the effective DEK, thus

ID	Threat
	providing unauthorized access to the previously unknown plaintext on the storage device.
T.UNAUTHORIZED_DATA_ACCESS	The cPP addresses the primary threat of unauthorized disclosure of protected data stored on a storage device. If an adversary obtains a lost or stolen storage device (e.g., a storage device contained in a laptop or a portable external storage device), they may attempt to connect a targeted storage device to a host of which they have complete control and have raw access to the storage device (e.g., to specified disk sectors, to specified blocks).
T.UNAUTHORIZED_FIRMWARE_MODIFY/EE	An attacker attempts to modify the firmware in the SED via a command from the AA or from the host platform that may compromise the security features of the TOE.
T.UNAUTHORIZED_FIRMWARE_UPDATE/EE	An attacker attempts to replace the firmware on the SED via a command from the AA or from the host platform with a malicious firmware update that may compromise the security features of the TOE.
T.UNAUTHORIZED_UPDATE	Threat agents may attempt to perform an update of the product which compromises the security features of the TOE. Poorly chosen update protocols, signature generation and verification algorithms, and parameters may allow attackers to install software and/or firmware that bypasses the intended security features and provides them unauthorized access to data.

5.3 Clarification of Scope

The evaluation of security functionality and scope are inherently tied to the specific assurance activities performed and the defined scope of the evaluation methodology. This evaluation provides no assurance that the TOE counters any threats which are not identified in the above PPs. 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 level of assurance for this evaluation is defined within the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019. (FDE_AA) and collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 (FDE_EE).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific device models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following document is provided with the product by the developer to the consumer and were evaluated along with the TOE:

- Archon Linux Unified Key Setup (LUKS) v3.0.0.2 Common Criteria User Guidance v2.8, May 2025. [AGD]

Any additional documentation provided with the product or may be 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. To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download documentation from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in ETR for Archon Linux Unified Key Setup (LUKS), which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

7.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

7.2 Evaluation Team Independent Testing

The Evaluation Team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019, FDE_AA) and collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 (FDE_EE). The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE is a software TOE and has been evaluated on the following host platforms.

Table 4: Archon Linux Unified Key Setup (LUKS) v3.0.0.2 Hardware Platforms (EUDs)

Vendor	TOE's Model	CPU	CPU Microarchitecture	CPU Family
Dell Inc.	Latitude 5430	12th Gen Intel® Core™ i7-1265U	Golden Cove	Alder Lake
	Precision 3260	12th Gen Intel® Core™ i7-12700	Golden Cove	Alder Lake
	Precision 3570	12th Gen Intel® Core™ i7-1265U	Golden Cove	Alder Lake
	Precision 5570	12th Gen Intel® Core™ i7-12700	Golden Cove	Alder Lake
	Latitude 5440	13th Gen Intel® Core™ i5-1335U	Raptor Cove	Raptor Lake
	Latitude 5540	13th Gen Intel® Core™ i5-1335U	Raptor Cove	Raptor Lake
	Precision 3580	13th Gen Intel® Core™ i5-1355U	Raptor Cove	Raptor Lake
	Precision 3590	Intel® Core™ Ultra 7 155U	Ultra/Redwood Cove	Meteor Lake

8.2 Excluded Functionality

The following product functionality is not included in the CC evaluation:

- The TOE only supports a CLI interface; no GUI or program, or script.

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) and the ETR. 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 Rev. 5 and CEM version 3.1 Rev. 5. The evaluation determined the TOE Name to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

The Evaluation Team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Archon Linux Unified Key Setup (LUKS) that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019. (FDE_AA) and collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 (FDE_EE).

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, and that the conclusion reached by the Evaluation Team was justified.

9.2 Evaluation of Development Documentation

The Evaluation Team applied each ADV CEM work unit. The Evaluation Team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019. (FDE_AA) and collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 (FDE_EE) related to the examination of the information contained in the TOE Summary Specification.

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 Assurance Activities, and that the conclusion reached by the Evaluation Team was justified.

9.3 Evaluation of Guidance Documents

The Evaluation Team applied each AGD CEM 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. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019. (FDE_AA) and collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 (FDE_EE) related to the examination of the information contained in the operational guidance documents.

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 Assurance Activities, and that the conclusion reached by the Evaluation Team was justified.

9.4 Evaluation of Life Cycle Support Activities

The Evaluation Team applied each ALC CEM work unit. The Evaluation Team found that the TOE was identified.

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, and that the conclusion reached by the Evaluation Team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The Evaluation Team applied each ATE CEM work unit. The Evaluation Team ran the set of tests specified by the Assurance Activities in the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019. (FDE_AA) and collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 (FDE_EE) and recorded the results in a Test Report, summarized in the ETR and AAR.

The Validation Team reviewed the work of the Evaluation Team and found that sufficient evidence was provided by the Evaluation Team to show that the evaluation activities addressed the test activities in the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019. (FDE_AA) and collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 (FDE_EE), and that the conclusion reached by the Evaluation Team was justified.

9.6 Vulnerability Assessment Activity

The Evaluation Team applied each AVA CEM work unit. The Evaluation Team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The Validattion 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 addressed the vulnerability analysis Assurance Activities in the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019. (FDE_AA) and collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 (FDE_EE), 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 are met. Additionally, the Evaluation Team's test activities also demonstrated the accuracy of the claims in the ST.

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 collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019 (FDE_AA) and collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 (FDE_EE), and correctly verified that the product meets the claims in the ST.

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 Archon Linux Unified Key Setup (LUKS) v3.0.0.2 Guidance v2.8, May 2025. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by SFRs claimed in the ST. All other functionality provided by the TOE, including the functionality defined in section 8.2 of this VR, needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained. Evaluation activities are strictly bound by the assurance activities described in the FDE_EE and FDE_AA cPPs and their accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Annexes

Not applicable.

12 Security Target

Archon Linux Unified Key Setup (LUKS) v3.0.0.2 Security Target v2.10, May 13, 2025. [ST]

13 Glossary

The following definitions are used throughout this document:

- **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.
- **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.

14 Bibliography

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

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition v2.0e + Errata 20190201, February 1, 2019.
6. Collaborative Protection Profile for Full Drive Encryption – Encryption Engine v2.0e + Errata 20190201, February 1, 2019.
7. Archon Linux Unified Key Setup (LUKS) v3.0.0.2 Security Target, Version 2.10, May 13, 2025. (ST)
8. Assurance Activity Report for Archon Linux Unified Key Setup (LUKS) v3.0.0.2, Version 2.2, May 8, 2025. (AAR)
9. CACI Archon Linux Unified Key Setup (LUKS) v3.0.0.2 Common Criteria User Guidance, Version 2.8, May 2025. (AGD)
10. CACI Archon OS v3.0.0.2 Common Criteria User Guidance, Version 1.2, July 2024 (Can be obtained from the NIAP PCL (www.niap-ccevs.org) posting VID11429). (OS AGD)
11. Evaluation Technical Report for Archon Linux Unified Key Setup (LUKS) v3.0.0.2, Version 1.9, May 13, 2025. (ETR)
12. Key Management Description Archon Linux Unified Key Setup (LUKS) v3.0.0.2, Version 0.6, April 22, 2025. (KMD)