National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1

Report Number: CCEVS-VR-VID11592-2026

Dated: 01/08/2026

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

Jenn Dotson

Lisa Mitchell

Lori Sarem

The MITRE Corporation

Common Criteria Testing Laboratory

Elliot Keen

Shyam Sundar Krishnamurthy

Joan Marshall

Acumen Security, LLC

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) Validation team's assessment of the evaluation of TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1 provided by Ampex Data Systems Corporation. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (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.

The evaluation was performed by Acumen Security Common Criteria Testing Laboratory (CCTL) and was completed in January 2026. 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:

- *PP-Configuration for Full Drive Encryption – Authorization Acquisition and Full Drive Encryption – Encryption Engine*, Version: 1.0 (CFG_CPP_FDE_AA-CPP_FDE_EE_V1.0) which includes the following components:
    - Base-PP: *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition*, Version 2.0 + Errata 20190201, February 1, 2019 (FDE_AA) and
    - Base-PP: *collaborative Protection Profile for Full Drive Encryption – Encryption Engine*, Version 2.0 + Errata 20190201, February 1, 2019 (FDE_EE).

The TOE is TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1. 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) 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. The Validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1 Security Target*, Version 1.20, 7 January 2026, and analysis performed by the Validation team.

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) 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, 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 (PP) 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	TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1
Protection Profile	*PP-Configuration for Full Drive Encryption – Authorization Acquisition and Full Drive Encryption – Encryption Engine*, Version: 1.0 (CFG_CPP_FDE_AA-CPP_FDE_EE_V1.0) which includes the following: • Base-PP: *collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition*, Version 2.0 + Errata 20190201, February 1, 2019 • Base-PP: *collaborative Protection Profile for Full Drive Encryption - Encryption Engine*, Version 2.0 + Errata 20190201, February 1, 2019
Security Target	*TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1 Security Target*, Version 1.20, 7 January 2026
Evaluation Technical Report	*Evaluation Technical Report for TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1*, Version 0.5, 01/07/2026
CC Version	Version 3.1, Revision 5, April 2017
CEM	*Common Methodology for Information Technology Security Evaluation: Evaluation Methodology*, Version 3.1, Revision 5, April 2017.
Conformance	CC Part 2 Extended and CC Part 3 Conformant

Item	Identifier
Result	
Sponsor and Developer	Ampex Data Systems Corporation
Evaluation Personnel	Elliot Keen, Shyam Sundar Krishnamurthy, Joan Marshall
CCEVS Validators	Jenn Dotson, Lisa Mitchell, Lori Sarem

3 Architectural Information

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

The TOE is an Authorization Acquisition (AA) module and Encryption Engine (EE) module for the Ampex TuffServ® Full Drive Encryption (FDE) solution protecting sensitive data at rest. It implements the data encryption, policy enforcement, and key management functions of the file server. User data is encrypted by the TOE prior to being forwarded to the attached drives for storage and decrypted when retrieved from the drives. Both the encryption and the decryption occur without user intervention and cannot be disabled.

Communicating with the iECDL for management and control can be done remotely via an RJ45 connector used for system control via Ethernet. In addition, the iECDL can be controlled directly via serial port connection. The iECDL supports two management applications: the iECDL Graphical User Interface (GUI) and iECDL Command Line Interface (CLI). The LAN (Local Area Network) provides the GUI interface and the serial port provides the CLI interface. Figure 1 shows the available ports.

Figure 1: Ampex Data Systems TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1

Internally, an iECDL contains two CPU (Central Processing Unit) cards: The Host System Card and the TuffServ® Encryption Module (TSEM). The Host System Card runs the Ampex Computing Platform (ACCE) software. The ACCE provides the Full Drive Encryption (FDE) Authorization Acquisition (AA) functionality. The TSEM provides the Encryption Engine (EE) FDE functionality.

The Host system provides the management interfaces to the GUI and the CLI, interacts with the two USB (Universal Serial Bus) devices that store the authentication factors that enable users to access the encrypted drives, and provides a bridge between the authentication storage devices and the TSEM. The TSEM provides the interface between the Host System card and the storage devices. The TSEM provides cryptographic key management services for the TuffServ® secure storage device. It is responsible for authenticating the authentication factors and encrypting and decrypting the user data. The two cards communicate with each over a USB connection.

AES-XTS (Advanced Encryption Standard- XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing) is implemented on the FPGA (Field Programmable Gate Array) and uses DEKs (Data Encryption Key) derived from BEV (Border Encryption Value) for encrypting the user data stored on the attached drive and for decrypting it when retrieved. The FPGA is resident on the TSEM card.

The iECDL supports the following four external storage devices. Two, the Key Transfer Device (KTD) and the cRSM (compact Removable Storage Media), are used for input of the authentication factor. The Authentication Factor determines if iECDL User and Administrator can access the protected data. The other two, the Removable Storage Media (RSM) and the intelligent Removable Storage Media (iRSM) are used to hold the data that is being encrypted.

The ST should be consulted for additional information each of the components.

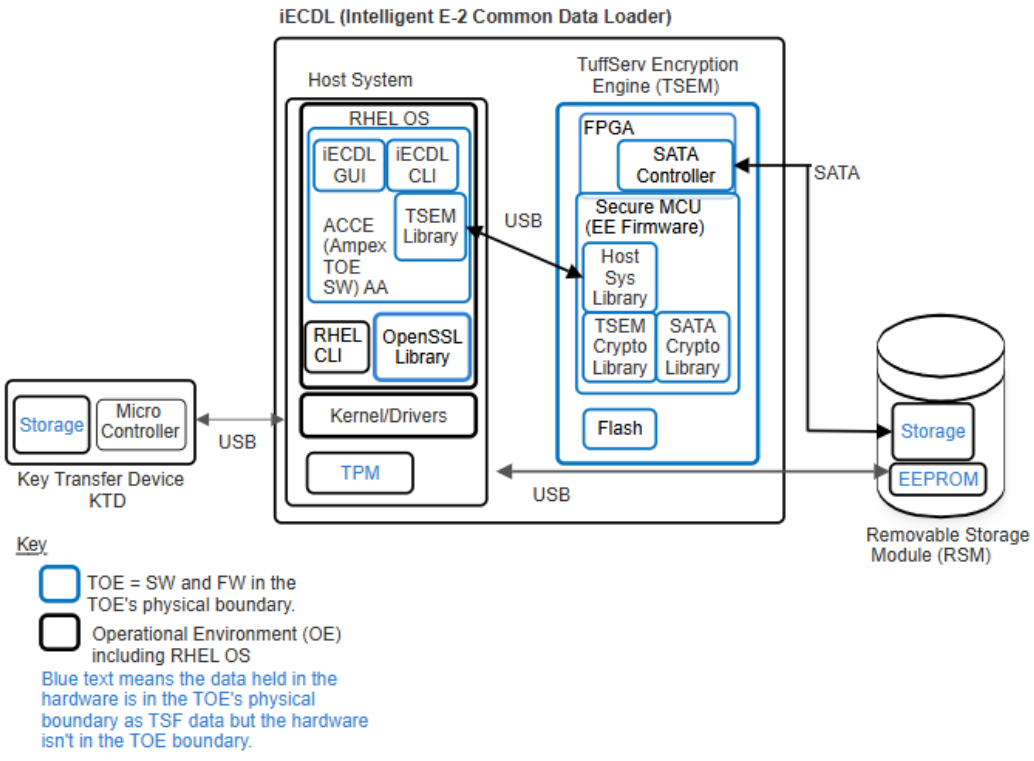
3.1 Evaluated Configuration

In the evaluated configuration, the TOE is configured with a RSM as the storage media, a KTD and a cRSM as the input devices for the authentication factors.

3.2 Physical Boundary

Figure 2 illustrates a typical iECDL with a KTD and an RSM. As noted with the diagram, components included in the TOE's physical boundary are identified in blue. Operational Environment components are identified in black.

Figure 2: iECDL TOE Components



In addition, a workstation is required to manage the iECDL. The workstation must be connected to the same LAN as the iECDL. The workstation must have the latest versions of Chrome or Edge browser installed.

3.3 Excluded Functionality

The following functionality is not in the scope of the evaluation:

- LEDs (Light Emitting Diode) on the front panel of the TOE are not included in the evaluation activities.
- The network interface used by the TOE Users and the supported network application protocols that access the iECDL memory (File Network File System (NFS), Secure Copy Protocol (SCP), Trivial File Transfer Protocol (TFTP), and Secure Shell (SSH)) are not included in the evaluated configuration.
- When the iECDL boots, there is a packet exchange between the KTD (Key Transfer Device) and the TPM (Trusted Platform Module). The purpose is to "trust" the KTD. This exchange or level of security is not included in the evaluation. All KTDs are considered trusted.
- Users (non-Administrator) access the TOE's protected data via File Network File System (NFS), Secure Copy Protocol (SCP), Trivial File Transfer Protocol (TFTP), and Secure Shell (SSH). The TOE supports the roles provided and managed by the RHEL Operating System (Operational Environment), allowing Users with privilege (superuser or root) access to files and applications stored on the protected disk, whereas non-privileged users will be denied access. This level of user roles, that determine which users have access to which data, is not included in the evaluated configuration.
- The iECDL provides an additional layer of security on top of the RHEL role-based security implemented. Upon login, the iECDL ensures that the User is allowed to invoke the specific command. This upper level of security is not included in the evaluation.
- Cryptographic Officer (CO)

4 Security Policy

This section summarizes the security functionality of the TOE:

4.1 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 AES-XTS-256 mode.

4.2 Security Management

The TOE supports management functions for changing and erasing the DEK using the iECDL GUI (Graphical User Interface) and initiating the TOE updates using the iECDL command line interface (CLI).

4.3 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).

4.4 Cryptographic Support

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

5 Assumptions and Clarification of Scope

5.1 Assumptions

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

- *collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition*, Version 2.0 + Errata 20190201, February 1, 2019
- *collaborative Protection Profile for Full Drive Encryption - Encryption Engine*, Version 2.0 + Errata 20190201, February 1, 2019

That information has not been reproduced here. CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E should be consulted if there is interest in that material.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionalities need 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 clarification. 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 assurance activities specified in CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E 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.
- Apart from the Admin Guide identified in Section 6, additional customer documentation for the specific 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.
- 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

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

- *TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1 Common Criteria User Guide,* Version 1.5, January 2026

All documentation delivered with the product is relevant to and within the scope of the TOE. This document is the only documentation that should be trusted to set-up, administer, or use the product in the evaluated configuration. Additional documentation was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device as evaluated.

7 IT Product Testing

This section describes the testing efforts of the Evaluation team. It is derived from information contained in *Assurance Activity Report for TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1*, Version 0.5, 01/07/2026 (AAR). The AAR provides an overview of testing and the prescribed evaluation 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 conducted independent testing at Ampex in Las Cruces, New Mexico in November 2025. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

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.

The Evaluation team used the Protection Profile 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 and the evaluation team verified that each test passed.

8 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 Evaluation Technical Report (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 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Evaluation Activities specified in CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E and their supporting documents.

8.1 Evaluation of Security Target (ASE)

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 TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1 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, and that the conclusion reached by the Evaluation team was justified.

8.2 Evaluation of Development Documentation (ADV)

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 and Guidance document. Additionally, the Evaluation team performed the Evaluation Activities related to the examination of the information contained in the TOE Summary Specification (TSS).

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.

8.3 Evaluation of Guidance Documents (AGD)

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 guide was 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, and that the conclusion reached by the Evaluation team was justified.

8.4 Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM 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, and that the conclusion reached by the Evaluation team was justified.

8.5 Evaluation of Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the Test Evaluation Activities in the CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E and recorded the results in the DTR, summarized in the AAR.

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.

8.6 Vulnerability Assessment Activity (AVA)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *Vulnerability Assessment for TuffServ® Intelligent E-2 Common Data Loader (iECDL) 2.74.1*, Version .5, January 5, 2026, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities was last conducted on January 5, 2026, and did not uncover any residual vulnerability.

The Evaluation team searched:

- 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
- CISA Known Exploited Vulnerabilities Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)
- US-CERT: http://www.kb.cert.org/vuls/html/search

The Evaluation team performed a search using the following keywords:

- TuffServ® Intelligent E-2 Common Data Loader
- iECDL

- Ampex Data Systems Corporation
- TuffServ Encryption Engine
- TSEM
- Data Encryption Key
- cRSM
- iRSM
- RSM
- KTD
- Ampex Computing Platform
- ACCE
- Infineon SLB9665XT2.0
- TSEM Cryptographic Library v1.1.16.0
- IPC-BL120B-ZM
- AMPEX OpenSSL Cryptographic Module v1.1.1
- IntelliProp Lycan FPGA
- NXP Kinetis K81
- BEV
- OpenSSL 1.1.1k
- Intel Atom C3558
- Disk encryption
- Key destruction
- Password caching
- Key sanitization

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.

8.7 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 followed the procedures defined in the CEM and performed the Evaluation Activities in CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E, and their supporting documents and correctly verified that the product meets the claims in the ST.

9 Validator Comments & Recommendations

The Validation team notes that the functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. This includes any claims made regarding Commercial Solutions for Classified (CSfC) implementations. Any claims made regarding CSfC should be verified with the CSfC program office. In addition, as noted in Section 3.3, protocols, such as SSH, have not been included in the evaluation and no claim can be made regarding their security implementation. Other functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. For example, the RSM/iRSM were not tested as they were used for data storage and are external to the TOE. No versions of the TOE and software, either earlier or later, were evaluated.

The evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section **Error! Reference source not found.** of this VR. Consumers are encouraged to download the configuration guides 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 should not be relied upon when configuring or operating the device as evaluated.

10 Annexes

Not applicable.

11 Security Target

TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1 Security Target, Version 1.20, 7 January 2026

12 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.

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 and General Model, CCMB-2017-04-001*, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002*, Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003*, Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
5. *PP-Configuration for Full Drive Encryption – Authorization Acquisition and Full Drive Encryption – Encryption Engine*, Version: 1.0 (CFG_CPP_FDE_AA-CPP_FDE_EE_V1.0).
6. *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, v2.0 + Errata 20190201*, February 1, 2019
7. *collaborative Protection Profile for Full Drive Encryption – Encryption Engine, v2.0 + Errata 20190201*, February 1, 2019
8. *Assurance Activity Report for TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1*, v0.5, 01/07/2026
9. *Evaluation Technical Report for TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1*, v0.5, 01/07/2026
10. *TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1 Common Criteria User Guide*, v1.5, January 2026
11. *TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1 Security Target*, v1.20, 07 January 2026
12. *Key Management Description TuffServ® Intelligent E-2 Common Data Loader (iECDL) v2.74.1*, Version 2.2, 07 January 2026
13. *Vulnerability Assessment for TuffServ® Intelligent E-2 Common Data Loader (iECDL) 2.74.1*, Version .5, January 5, 2026
14. *Test Plan for TuffServ® Intelligent E-2 Common Data Loader (iECDL) 2.74.1*, Version .1.5, 01/07/2026