

**National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme**



Validation Report

**Curtiss-Wright Defense Solutions XMC NVMe Encryptor
version 1.0.0**

Report Number: CCEVS-VR-VID11505-2024
Dated: November 5, 2024
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
David Thompson

The Aerospace Corporation

Common Criteria Testing Laboratory

Yoel Fortaleza
John Messiha

*Gossamer Security Solutions, Inc.
Columbia, MD*

Table of Contents

1	Executive Summary.....	1
2	Identification.....	1
3	Architectural Information.....	2
3.1	TOE Description.....	3
3.2	TOE Architecture	3
3.3	Physical Boundaries	3
4	Security Policy.....	3
4.1	Cryptographic support	3
4.2	User data protection.....	3
4.3	Security management	3
4.4	Protection of the TSF.....	4
5	Assumptions & Clarification of Scope.....	4
6	Documentation	5
7	IT Product Testing.....	5
7.1	Developer Testing	5
7.2	Evaluation Team Independent Testing.....	5
8	Results of the Evaluation.....	5
8.1	Evaluation of the Security Target (ASE).....	6
8.2	Evaluation of the Development (ADV).....	6
8.3	Evaluation of the Guidance Documents (AGD).....	6
8.4	Evaluation of the Life Cycle Support Activities (ALC).....	7
8.5	Evaluation of the Test Documentation and the Test Activity (ATE).....	7
8.6	Vulnerability Assessment Activity (VAN)	7
8.7	Summary of Evaluation Results	7
9	Validator Comments/Recommendations.....	8
10	Annexes	Error! Bookmark not defined.
11	Security Target	8
12	Glossary	8
13	Bibliography	9

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Curtiss-Wright Defense Solutions XMC NVMe Encryptor version 1.0.0 Hardware Encryption Layer solution provided by Curtiss-Wright Defense Solutions. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in November 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. 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 - Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 and collaborative Protection Profile for Full Drive Encryption Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019.

The Target of Evaluation (TOE) is the Curtiss-Wright Defense Solutions XMC NVMe Encryptor version 1.0.0.

The TOE identified in this Validation Report 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). This Validation Report 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 evaluation technical report 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 evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Curtiss-Wright Defense Solutions XMC NVMe Encryptor version 1.0.0 Security Target, Version 0.5, November 1, 2024 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 Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The evaluation conformance result.
- 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	Curtiss-Wright Defense Solutions XMC NVMe Encryptor version 1.0.0
Protection Profile	collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 and collaborative Protection Profile for Full Drive Encryption Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019
ST	Curtiss-Wright Defense Solutions XMC NVMe Encryptor version 1.0.0 Security Target, Version 0.5, November 1, 2024
Evaluation Technical Report	Evaluation Technical Report for Curtiss-Wright Defense Solutions XMC NVMe Encryptor version 1.0.0, Version 0.3, November 1, 2024
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Curtiss-Wright Defense Solutions
Developer	Curtiss-Wright Defense Solutions
Common Criteria	Gossamer Security Solutions, Inc.
Testing Lab (CCTL)	Columbia, MD
CCEVS Validators	Jerry Myers and David Thompson, of The Aerospace Corporation.

3 Architectural Information

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

The TOE is Curtiss-Wright Defense Solutions XMC NVMe Encryptor version 1.0.0.

The TOE provides hardware Full Drive Encryption of standard NVMe compliant drives.

3.1 TOE Description

The Curtiss-Wright Defense Solutions XMC NVMe Encryptor (hereafter referred to as the TOE) is an in-line hardware encryption layer that is used for Data-At-Rest (DAR) encryption of attached NVMe drives and can be installed in any host system that supports installation of the assembly.

To comply with NIAP Technical Decision 606 the TOE must be managed using the serial cable or by using SSH over a private, dedicated network.

3.2 TOE Architecture

The TOE provides a hardware Full Drive Encryption solution that can encrypt standard NVMe compliant drives.

3.3 Physical Boundaries

The TOE's physical boundary is the physical perimeter of its enclosure. The TOE provides a ruggedized solution to secure Data at Rest (DAR).

4 Security Policy

This section summarizes the security functionality of the TOE:

1. Cryptographic support
2. User data protection
3. Security management
4. Protection of the TSF

4.1 Cryptographic support

The TOE includes cryptographic functionality for key management, user authentication, and block-based encryption including symmetric key generation, encryption/decryption, cryptographic hashing, keyed-hash message authentication, and password-based key derivation. These functions are supported with suitable random bit generation, key derivation, salt generation, initialization vector generation, secure key storage, and key destruction. These primitive cryptographic functions are used to encrypt Data-At-Rest (including the generation and protection of keys and key encryption keys) used by the TOE.

4.2 User data protection

The TOE performs Full Drive Encryption on the entire drive (so that no plaintext exists) and does so without user intervention.

4.3 Security management

The TOE provides each of the required management services necessary to manage the full drive encryption using a command line interface.

4.4 Protection of the TSF

The TOE implements a number of features to protect itself to ensure the reliability and integrity of its security features. It protects key and key material and includes functions to perform self-tests and software/firmware integrity checking so that it might detect when it is failing or may be corrupt. If any of the self-tests fails, the TOE will not go into an operational mode.

5 Assumptions & Clarification of Scope

Assumptions

The Security Problem Definition, including the assumptions, may be found in the following Protection Profile (PP) documents. These PPs are collectively referred to as the FDEAAcPP20E/FDEEEcPP20E.

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

The complete security problem has not been reproduced here and the FDEAAcPP20E/FDEEEcPP20E should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the FDEAAcPP20E/FDEEEcPP20E 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.

Clarification of scope

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 with a certain level of assurance (the assurance activities specified in the Full Drive Encryption Protection Profiles and performed by the evaluation team).
- 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 Full Drive Encryption 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 FDEAAcPP20E/FDEEEcPP20E and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- Curtiss-Wright NVMe Encryptor User Guide, DDOC0182-000-NIAP A2

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.

6.1 TOE Evaluated Configuration

The TOE is the Curtiss-Wright Defense Solutions XMC NVMe Encryptor, an in-line hardware encryption layer that is used for Data-At-Rest (DAR) encryption of attached NVMe drives and can be installed in any host system that supports installation of the assembly.

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 the configuration guides 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 the proprietary Detailed Test Report for Curtiss-Wright Defense Solutions XMC NVMe Encryptor version 1.0.0, Version 0.2, October 18, 2024 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

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 a Common Criteria Certification document and ran the tests specified in the FDEAAcPP20E/FDEEEcPP20E, including the tests associated with optional requirements. The AAR, in Sections 1.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

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 ETR. The reader of this document can assume that all assurance 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 Curtiss-Wright Defense Solutions XMC NVMe Encryptor version 1.0.0 TOE to be Part 2 extended, and to meet the SARs contained in the FDEAAcPP20E/FDEEEcPP20E.

8.1 Evaluation of the 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 Curtiss-Wright Defense Solutions XMC NVMe Encryptor version 1.0.0 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators 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 the Development (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 Security Target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the FDEAAcPP20E/FDEEEcPP20E related to the examination of the information contained in the TOE Summary Specification (TSS) section of the ST.

The validators 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 the 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. All the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided 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 the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided 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 the 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 assurance activities in the FDEAAcPP20E/FDEEEcPP20E and recorded the results in a Test Report, summarized in the AAR.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided 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 (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (<https://web.nvd.nist.gov/view/vuln/search>) and Vulnerability Notes Database (<http://www.kb.cert.org/vuls/>) on 10/15/2024 with the following search terms: "NVMe Encryptor", "Linux 8.9", "drive encryption", "disk encryption", "key destruction", "key sanitization", "Key caching", "Opal management software", "SED management software", "Password caching", "Curtiss Wright", "Curtiss Wright Crypto Firmware", "ARM7", "LPC4333", "ATECC608B", "FM24V05-G", "Xilinx", "XCKU085 FPGA", "AES-XTS". The public search for vulnerabilities did not uncover any residual vulnerabilities.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided 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 testing 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 correctly verified that the product meets the claims in the ST.

9 Validator Comments/Recommendations

All validator comments and recommendations are adequately addressed in the Assumptions and Clarification of Scope section.

10 Security Target

The Security Target is identified as: *Curtiss-Wright Defense Solutions XMC NVMe Encryptor version 1.0.0 Security Target, Version 0.5, November 1, 2024.*

11 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.

12 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, April 2017.
- [2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
- [3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
- [4] collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019.
- [5] collaborative Protection Profile for Full Drive Encryption Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019.
- [6] Curtiss-Wright Defense Solutions XMC NVMe Encryptor version 1.0.0 Security Target, Version 0.5, November 1, 2024 (ST).
- [7] Assurance Activity Report for Curtiss-Wright Defense Solutions XMC NVMe Encryptor version 1.0.0, Version 0.3, November 1, 2024 (AAR).
- [8] Detailed Test Report for Curtiss-Wright Defense Solutions XMC NVMe Encryptor version 1.0.0, Version 0.2, October 18, 2024 (DTR).
- [9] Evaluation Technical Report for Curtiss-Wright Defense Solutions XMC NVMe Encryptor version 1.0.0, Version 0.3, November 1, 2024 (ETR)