National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer

Report Number: **CCEVS-VR-10862-2018**
Dated: **August 21, 2018**
Version: **1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

John Butterworth
Joanne Fitzpatrick
Stelios Melachrinoudis
The MITRE Corporation
Bedford, MA

Kenneth Stutterheim
The Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Tammy Compton
Gossamer Security Solutions, Inc.
Catonsville, MD

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 to determine the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), (which is where specific security claims are made) as well as this Validation Report (VR) (which describes how those security claims were evaluated, tested, and any restrictions that may be imposed upon the evaluated configuration) to help in that determination. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 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 Curtiss-Wright Data Transport System 1-Slot Software Encryption Layer solution provided by Curtiss-Wright Defense Solutions. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied. This VR applies only to the specific version and configurations of the product as evaluated and as documented in the ST.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in August 2018. The information in this report is largely derived from the proprietary Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. Those are summarized in the Assurance Activity Report (AAR) for this evaluation. 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, 09 September 2016 and collaborative Protection Profile for Full Drive Encryption Authorization Acquisition, Version 2.0, 09 September 2016.

The Target of Evaluation (TOE) is the Curtiss-Wright Data Transport System 1-Slot Software Encryption Layer.

The Target of Evaluation (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 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). 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 of 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 Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer (FDEEEcPP20/FDEAAcPP20) Security Target, Version 0.7, August 14, 2018 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 Product Compliant List (PCL).

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 conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Curtiss-Wright Data Transport System 1-Slot Software Encryption Layer (Specific models identified in Section 8)
Protection Profile	collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0, 09 September 2016 and collaborative Protection Profile for Full Drive Encryption Authorization Acquisition, Version 2.0, 09 September 2016
ST	Curtiss-Wright Data Transport System 1-Slot Software Encryption Layer Security Target, Version 0.7, August 14, 2018
Evaluation Technical Report	Evaluation Technical Report for Curtiss-Wright Data Transport System 1-Slot Software Encryption Layer, version 0.3, August 14, 2018

Item	Identifier
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Curtiss-Wright Defense Solutions
Developer	Curtiss-Wright Defense Solutions
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Catonsville, MD
CCEVS Validators	John Butterworth, ECR Team, The MITRE Corporation Joanne Fitzpatrick, ECR Team, The MITRE Corporation Stelios Melachrinoudis, Lead Validator, The MITRE Corporation Kenneth Stutterheim, Senior Validator, The Aerospace Corporation

3 Architectural Information

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

The Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Layer (hereafter referred to as the TOE) is a software encryption layer that is used for Data-At-Rest (DAR) encryption as part of the underlying rugged Network Attached Storage (NAS) file server, denoted as the Curtiss-Wright DTS1 CSFC/ECC Cryptographic Data Transport System (DTS) (hereafter referred to as the DTS1). The underlying DTS1 is intended for use in Unmanned Aerial Vehicles (UAV), Unmanned Underwater Vehicles (UUV), and Intelligence Surveillance Reconnaissance (ISR) aircraft. The TOE operates at, and is evaluated at, the firmware level. Easily integrated into network centric systems, the DTS1 is an easy to use, turnkey, rugged network File Server that houses one Removable Memory Cartridge (RMC) that provides quick off load of data. The RMC can be easily removed from one DTS1 and installed into any other DTS1 providing full, seamless data transfer between one or more networks in separate locations (e.g. ground => vehicle => ground).

3.1 TOE Evaluated Configuration

Detail regarding the evaluated configuration is provided in Section 8 below.

3.2 TOE Architecture

The TOE provides a software Full Drive Encryption solution that can accept a Removable Memory Cartridge (RMC) which contains a data drive.

3.3 Physical Boundaries

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

4 Security Policy

This section summaries 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 the management services required to manage the full drive encryption via a command line interface.

4.4 Protection of the TSF

The TOE implements functions 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 fail, the TOE will not enter an operational mode.

5 Assumptions & Clarification of Scope

Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0, 09 September 2016
- collaborative Protection Profile for Full Drive Encryption Authorization Acquisition, Version 2.0, 09 September 2016

That information has not been reproduced here and the FDEEEcPP20/FDEAAcPP20 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 FDEEEcPP20/FDEAAcPP20 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Any other functionality provided by the device 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 model and software as identified in this document, and not any earlier or later versions released or in process. More specifically, this evaluation only covers the software encryption layer of the Curtiss-Wright Data Transport Solution, not the hardware encryption layer, which is covered in a separate evaluation. It is assumed that the hardware encryption layer has been previously configured correctly according to the Administrative Guidance for the Data Transport Solution to verify testing performed using the software encryption layer.
- 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 FDEEEcPP20/FDEAAcPP20 and applicable TRRT Decisions and 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 DTS1 CSfC / ECC Cryptographic Data Transport System (Network File System) User Guide, DDOC0099-000-A2

To use the product in the evaluated configuration, the product must be configured as specified in this guide. Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device in its evaluated configuration. Consumers are encouraged to download the CC configuration guides directly 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 following proprietary document:

- *Evaluation Technical Report for Curtiss-Wright Data Transport System 1-Slot Software Encryption Layer*, Version 0.3, August 14, 2018

A non-proprietary summary of the test configuration, test tools, and tests performed may be found in:

- *Assurance Activity Report (FDEEEcPP20/FDEAAcPP20) for Curtiss-Wright Data Transport System 1-Slot Software Encryption Layer*, Version 0.3, August 14, 2018.

7.1 Developer Testing

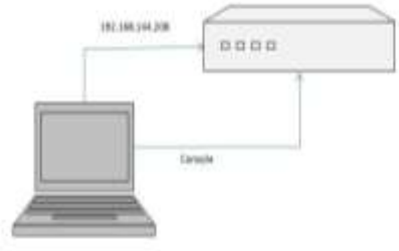
No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the FDEEEcPP20/FDEAAcPP20 including the tests associated with optional requirements.

7.3 Test Environment

TOE: Curtiss-Wright Defense Solutions Data Transport System 1-Slot (build 373)



7.4 Supporting Products

Windows 10, 64 bit

7.5 Software Tools

- Standard Windows utilities (e.g., notepad, snip tool)
- Putty version 0.67 (used to connect to the device)
- HxD (Hexeditor) version 1.7.7.0 (used to examine dumped memory files)
- Gossamer developed test tools
- Curtiss Wright tool for performing cryptographic operation to setup TOE – cm_crypto
- Lime version lime-3.10.0-693.el7 (used to dump memory)
- Wireshark

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 4 and CEM version 3.1 rev 4. The evaluation determined the Data Transport System 1-Slot Software Encryption Layer TOE to be Part 2 extended, and to meet the SARs contained in the FDEEEcPP20/FDEAAcPP20.

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 Data Transport System 1-Slot Software Encryption Layer product 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 FDEEEcPP20/FDEAAcPP20 related to the examination of the information contained in the TSS.

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 of 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 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 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 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 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 FDEEEcPP20/FDEAAcPP20 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 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 (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 included a public search for vulnerabilities. On July 23, 2018, the evaluator searched the National Vulnerability Database at (https://web.nvd.nist.gov/view/vuln/search) and the Vulnerability Notes Database at (http://www.kb.cert.org/vuls/) using the following search terms: "disk encryption", "drive encryption", "key destruction", "key sanitization", "Opal management software", "SED management software", "Password caching", "Key caching", "Curtiss Wright", "DTS1", "Defense Solutions Data Transport System", "Linux Unified Key Setup", "LUKS", "Libgcrypt", "openssl", "CentOS".

The public search for vulnerabilities did not uncover any residual vulnerability.

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.

8.7 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

The validators suggest that the consumer pay particular attention to the evaluated configuration of the software encryption layer. The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided, to include software, firmware, or hardware that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

In addition to the software/firmware-based FDE layer provided by the DTS1, the DTS1 provides a hardware-based Full Drive Encryption (FDE) layer to encrypt the drive within the RMC. The hardware-based FDE layer is addressed in a separate evaluation.

Administrators should pay particular attention to the encryptor's ability to setup Automatic Login covered in section 6.3.6 of the Administrative Guide. It is possible to set a command that will allow for saving login credentials, which when saved, allows for login to occur automatically during power up. If default passwords are used, they must be changed.

NIAP established the Full Drive Encryption Technical Rapid Response Team (FDE-TRRT) which, along with the Full Drive Encryption International Technical Community (FDE iTC), addressed questions and concerns related to evaluations claiming conformance to the *Protection Profile for Full Drive Encryption.* A Technical Decision is an issue resolution statement that clarifies or interprets protection profile requirements and assurance activities. The FDE-TRRT, in conjunction with the Full Drive Encryption (FDE) Interpretations Team (FIT), has formally posted eight Technical Decisions related to *collaborative Protection Profile for Full Drive Encryption- Encryption Engine* and *collaborative Protection Profile for Full Drive Encryption*

Authorization Acquisition: TD0229, TD0233, TD0308, TD0309, TD0310, TD0312, TD0344, TD0345 (see https://www.niap-ccevs.org/Documents_and_Guidance/view_tds.cfm). Of these, the following seven PSS-TRRT Technical Decisions applied to this evaluation: TD0229, TD0233, TD0308, TD0309, TD0312, TD0344, TD0345.

9.1 TRRT Decisions

There were five TRRT decisions made throughout the course of this evaluation, four that led to TDs:

9.1.1 Incompatible Key Destruction Requirements and Assurance Activities

A TRRT request was made to address multiple issues in FPT_PWR_EXT.1, FPT_PWR_EXT.2, FCS_CKM_EXT.4(b), and FCS_CKM_EXT.6:

There were several requirements (FPT_PWR_EXT.1, FPT_PWR_EXT.2, FCS_CKM_EXT.4(b)) where the Assurance Activity states to perform key destruction tests and/or include KMD documentation according to FCS_CKM.4(b). However, the FDE AA cPP does not have FCS_CKM.4(b) as one of the SFRs, so Assurance Activities referring to it cannot be performed. Additionally, the FDE EE cPP does have FCS_CKM.4(b), but it is selection-based, and the lab did NOT include FCS_CKM.4(b). Additionally, the Extended Component Definition (ECD) of FCS_CKM_EXT.6 instructs the ST author to select two FCS_CKM.4 iterations through an assignment, even though the ECD was intended for a PP author to instantiate accordingly. However, FCS_CKM_EXT.6 in the FDE EE cPP allows an ST author to include only a single FCS_CKM.4 iteration which, without clarification within the SFR, possibly violates the FCS_CKM_EXT.6 ECD.

Upon review, the FDE-TRRT and FIT agreed to resolve the problems raised and issue TD0345 with the explanation provided by the FIT via the following FDE Interpretation:

https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/FITDecision201806.pdf (accessed August 17, 2018)

9.1.2 Inconsistent FCS_CKM.4 and FCS_CKM_EXT.4 Key Destruction References

A TRRT request was made to address multiple inconsistencies in references to other requirements and test evaluation activities for multiple FCS_CKM.4 and FCS_CKM_EXT.4 iterations:

[In] the SD for cpp_fde_aa v2 FCS_CKM.4(a) Cryptographic Key Destruction (Power Management) is this: "Test: The test activities performed for this SFR are identical to those performed for FCS_CKM.4(a)."

But this is fcs_ckm.4(a). The reference is circular, with NO tests defined in the SD for fcs_ckm.4(a)

[And] for fcs_ckm_ext.4(a)Destruction timing: "There are no test evaluation activities for this SFR."

FCS_CKM_ext.4(b) "There are no test evaluation activities for this SFR."

FCS_CKM_ext.4(d) has tests for 3rd party storage.

I would think the text should be changed to link it to a test or changed to "there are no test evaluation activities for this SFR" which would bring it in line with the FDE_EE.

Upon review, the FDE-TRRT and FIT agreed to resolve the problems raised and issue TD0344 with the explanation provided by the FIT via the following FDE Interpretation:

https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/FITDecision201805.pdf (accessed August 17, 2018)

9.1.3 Hardware Test for FDP_DSK_EXT.1 Of A Firmware Solution

A TRRT request was made to clarify the Test Assurance Activity for FDP_DSK_EXT.1:

The Curtiss Wright Full Disk Encryption solution is named software but is [actually] a firmware product operating below the layer that comprises the software filesystem. Because of this, the evaluator chose the hardware test since it was most applicable to the product's functions. The evaluator performed the address operations on the blocks since that matches the implementation; was the choice of the hardware test and block access acceptable in this case?

The FDE-TRRT resolved this TRRT request by allowing the choice of the hardware test and block access if firmware was part of a physical solution. It did not lead to a TD or FDE Interpretation.

TRRT decisions that do not lead to a TD or FDE Interpretation only apply to this evaluation and are not to be used as precedent to future evaluations.

9.1.4 Validity of Selection for Key and Key Material Protection, FPT_KYP_EXT.1

A TRRT request was made to verify the validity of a "none" selection being made in FPT_KYP_EXT.1 for the following, despite the PP not offering the selection of none: *The TSF shall [only store keys in non-volatile memory when wrapped, as specified in FCS_COP.1(d), or encrypted, as specified in FCS_COP.1(g) or FCS_COP.1(e)], unless the key meets any one of following criteria [none].*

The FDE-TRRT agreed that "none" is a valid selection.

Upon review, the FDE-TRRT and FIT agreed to resolve the problems raised and issue TD0312 with the explanation provided by the FIT via the following FDE Interpretation:

https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/FITDecision201804.pdf (accessed August 21, 2018)

9.1.5 Unclear Enumeration of Selections in FPT_KYP_EXT.1

A TRRT request was made to clarify the enumeration of selections in FPT_KYP_EXT.1:

In both the FDE AA and FDE EE cPPs, it is unclear as to how many different selections (boldfaced) are referred to in the phrase, "The TSF shall ***[selection: not store keys in non-volatile memory, only store keys in non-volatile memory when wrapped, as specified in FCS_COP.1(d), or encrypted, as specified in FCS_COP.1(g) or FCS_COP.1(e)]****, unless the key meets any one of the following criteria...". It is customary to make the comma a delimiter to separate each selection, or if there are commas, semicolons as the delimiter, which creates this potential ambiguity.*

The FDE-TRRT agreed and stated that the selections should be: *[not store keys in non-volatile memory; only store keys in non-volatile memory when wrapped, as specified in FCS_COP.1(d); only store keys in non-volatile memory when encrypted, as specified in FCS_COP.1(g); only store keys in non-volatile memory when encrypted, as specified in FCS_COP.1(e)].*

Upon review, the FDE-TRRT and FIT agreed to resolve the problems raised and issue TD0312 with the explanation provided by the FIT via the following FDE Interpretation:

https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/FITDecision201804.pdf (accessed August 21, 2018)

10 Annexes

Not applicable

11 Security Target

The Security Target is identified as: *Curtiss-Wright Data Transport System 1-Slot Software Encryption Layer (FDEEEcPP20/FDEAAcPP20) Security Target, Version 0.7, August 14, 2018.*

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, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4] collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0, 09 September 2016

[5] collaborative Protection Profile for Full Drive Encryption Authorization Acquisition, Version 2.0, 09 September 2016.

[6] Curtiss-Wright Data Transport System 1-Slot Software Encryption Layer (FDEEEcPP20/FDEAAcPP20) Security Target, Version 0.7, August 14, 2018 (ST).

[7] Assurance Activity Report (FDEEEcPP20/FDEAAcPP20) for Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer, Version 0.3, August 14, 2018 (AAR).

[8] Detailed Test Report (FDEEEcPP20/FDEAAcPP20) for Curtiss-Wright Data Transport System 1-Slot Software Encryption Layer, Version 0.2, August 14, 2018 (DTR).

[9] Evaluation Technical Report for Curtiss-Wright Data Transport System 1-Slot Software Encryption Layer, Version 0.3, August 14, 2018 (ETR)

[10] DTS1 CSfC/ECC Cryptographic Data Transport System User Guide DDOC0099-000-A2