National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Enveil ZeroReveal® Compute Fabric Server v2.5.4

Report Number: CCEVS-VR-11151-2021

Dated: 05/28/2021

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

Marybeth Panock
Swapna Katikaneni
Ken Elliott
Jerome Myers
Aerospace Corporation

Common Criteria Testing Laboratory

Kenneth Lasoski

Rahul Joshi

Aruna Shaju K

Riya Thomas

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 Enveil ZeroReveal® Compute Fabric Server v2.5.4 (the Target of Evaluation, or 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 TOE is the ZeroReveal Compute Fabric Server (otherwise referred to as the ZeroReveal Server, or the TOE) software application which communicates to one or more instances of the ZeroReveal Client software application via REST over mutually authenticated TLS. The REST APIs may be used over HTTPS/TLS and require that the system communicating with the Server have at least once instance of the ZeroReveal Client software application installed. Users and applications communicate to the ZeroReveal Server through the REST APIs to retrieve data. An administrator interacts with and manages the ZeroReveal Server via configuration files (modifiable by a text editor) via the host platform. Note that the ZeroReveal Server does not provide a graphical user interface (GUI) or a command line interface (CLI). The TOE is evaluated as a software application only. Enveil ZeroReveal™ Compute Fabric contains functionality that is not covered by Protection Profile for Application Software. As with all evaluations claiming conformance to a NIAP-approved protection profile, only the functionality specified in the profile is evaluated. The TOE's homomorphic encryption techniques and the associated databases, including accessing, retrieving, storing, or operations on databases, are outside the scope of this evaluation. This evaluation makes no security claims about these features. Additionally, the ZeroReveal client software, which is required for the operation of the TOE, is outside the scope of this evaluation and was evaluated as another evaluation separately.

The evaluation was completed by Acumen Security in May 2021. The information in this report is largely derived from the Assurance Activities Report (AAR) and associated test reports authored by Acumen Security. The evaluation determined that the product is conformant with both Common Criteria Part 2 Extended and Part 3 Extended and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for

Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP] and Functional Package for Transport Layer Security (TLS), Version 1.1, dated 12 February 2019 [TLS-PKG].

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(AAs) contained in the Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP] and Functional Package for Transport Layer Security (TLS), Version 1.1, dated 12 February 2019 [TLS-PKG]. 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 Evaluation Technical Report (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 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 Protection Profile containing AAs, which are interpretations of the 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 Compliance 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 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	Enveil ZeroReveal® Compute Fabric Server v2.5.4
Protection Profile	Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP] and Functional Package for Transport Layer Security (TLS), Version 1.1, dated 12 February 2019 [TLS-PKG]
Security Target	Enveil ZeroReveal® Compute Fabric Server v2.5.4 Security Target
Evaluation Technical Report	Evaluation Technical Report for Enveil ZeroReveal® Compute Fabric Server v2.5.4
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Extended
Sponsor	Enveil, Inc.
Developer	Enveil, Inc
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd. #395 Rockville, MD 20850
CCEVS Validators	Marybeth Panock Swapna Katikaneni Ken Elliott

	Jerry Myers

3 Architectural Information

The TOE is Enveil ZeroReveal® Compute Fabric Server. The evaluated version of the TOE is 2.5.4.

The TOE is a software application which communicates to one or more instances of the ZeroReveal Client software application via REST over mutually authenticated TLS. The REST APIs may be used over HTTPS/TLS and require that the system communicating with the Server have at least once instance of the ZeroReveal Client software application installed. Note that the ZeroReveal Server does not provide a graphical user interface (GUI) or a command line interface (CLI). Users and applications communicate to the ZeroReveal Server through the REST APIs to retrieve data. An administrator interacts with and manages the ZeroReveal Server via configuration files (modifiable by a text editor) via the host platform.

The diagram below shows the parts of the TOE application, and how the evaluation security boundary is identified. The Client application is evaluated separately and is not part of this evaluation.

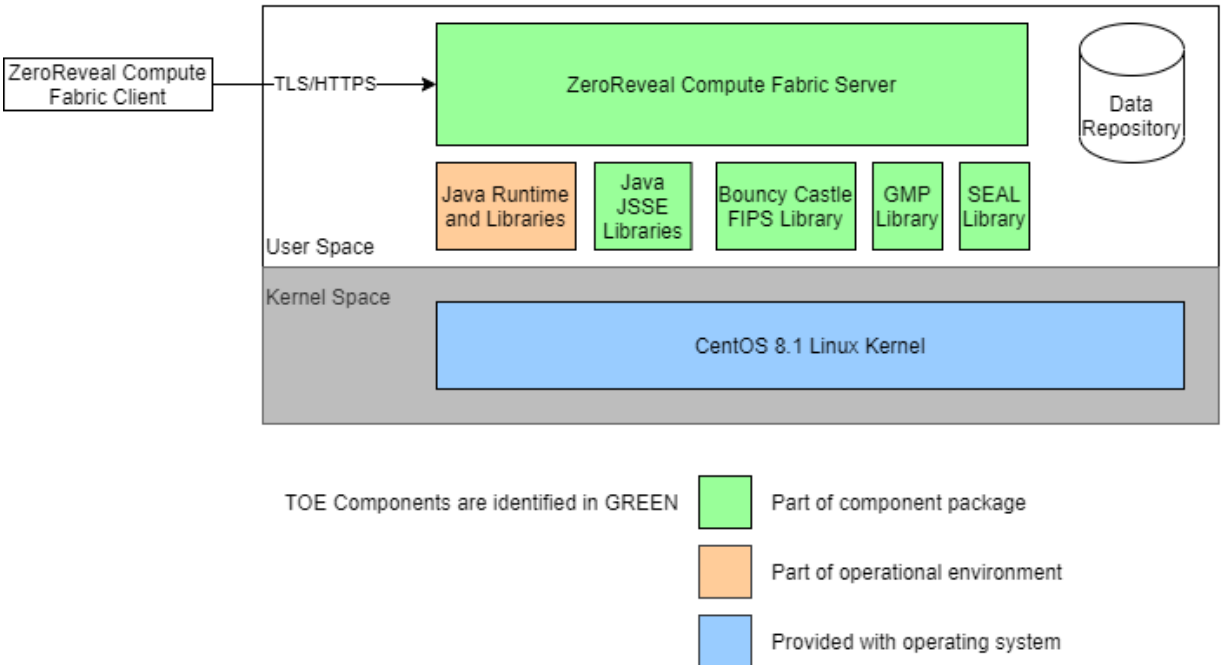

Figure 1 - TOE Operational Environment

4 Security Policy

The TOE provides the security functionality required by [SWAPP] and [TLS-PKG].

4.1 Cryptographic Support

The cryptographic services provided by the TOE are described below:

Cryptographic Method	Use within the TOE
AES-GCM	TLS encryption
ECDSA	TLS key generation, signature generation and verification
RSA	TLS key generation, signature generation and verification
HMAC	Message integrity and authentication for TLS
AES-CCM	Storage of credentials
DRBG	Random bit generation for all cryptographic functions

Table 2 TOE Provided Cryptography

Each of these cryptographic algorithms have been validated for conformance to the requirements specified in their respective standards, as identified below:

Algorithm	Standard	Mode/Keysize	CAVP Cert. #
HMAC_DRBG	NIST SP 800-90A	HMAC-SHA2-512 with 256 bits of entropy seeded by the platform DRBG	C1874
ECDSA KeyGen ECDH Key Establishment ECDSA SigGen/SigVer	FIPS Pub 186-4, Appendix B.4 NIST SP 800-56Arev3 FIPS Pub 186-4, Section 5	Curves P-256 and P-384	C1874
RSA KeyGen RSA SigGen/SigVer	FIPS Pub 186-4, Appendix B.3 FIPS Pub 186-4, Section 4	2048 bits	C1874
AES-GCM	NIST SP 800-38D	256 bits	C1874
AES-CCM	NIST SP 800-38C	256 bits	C1874
SHA2-256 SHA2-384 SHA2-512	FIPS Pub 180-4	Digest size 256 bits Digest size 384 bits Digest size 512 bits	C1874
HMAC-SHA2-256	FIPS Pub 198-1	Key size 256 bits, block size 512 bits, digest size 256 bits	C1874

Algorithm	Standard	Mode/Keysize	CAVP Cert. #
HMAC-SHA2-384		Key size 384 bits, block size 1024 bits, digest size 384 bits	
HMAC-SHA-512		Key size 512 bits, block size 1024 bits, digest size 512 bits	

Table 3 CAVP Algorithm Testing References

4.2 User Data Protection

The ZeroReveal Server network communication is restricted to user-initiated communication for responses to API requests from ZeroReveal Clients.

4.3 Identification and Authentication

The ZeroReveal server performs X.509v3 certificate validation functions to authenticate the certificate(s) during the establishment of the TLS trusted channel.

4.4 Security Management

An enterprise manages the TOE via configuration files on each installation platform. There is no management GUI, CLI, or interface to manage the TOE over the network.

The TOE does not include any predefined or default credentials and utilizes the platform recommended storage process for configuration files.

4.5 Privacy

The TOE does not collect or transmit Personally Identifiable Information (PII) over the network.

4.6 Protection of the TSF

The TOE leverages platform provided package management for secure installation and updates. The TOE installation package includes only those third-party libraries necessary for its intended operation. The TOE is designed to utilize compiler-provided anti-exploitation capabilities.

4.7 Trusted Path/Channels

The TOE communicates to the ZeroReveal® Compute Fabric Client via REST API over mutually authenticated TLS. Administrators configure the TOE via local access only, making changes to configuration files.

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.

The following assumptions are drawn directly from the [SWAPP]:

ID	Assumption
A.PLATFORM[1]	The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

Table 4 Assumptions

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.

The following threats are drawn directly from the [SWAPP]:

ID	Threat
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.

Table 5 Threats

[1] This Assumption is modified by TD0427.

5.3 Clarification of Scope

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 PP_APP_v1.3 and PKG_TLS_V1.1.
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- Consistent with the expectations of the Protection Profile, 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. This includes:
    - Databases, including accessing, retrieving, storing, or operations on databases.
    - The homomorphic encryption process, including the algorithms, uses and the security strength of the resultant ciphertext.

6 Documentation

The following document is available for downloading from the NIAP web site. It should be considered to be delivered with the TOE:

- Enveil ZeroReveal® Compute Fabric Configuration Guide for Common Criteria v3.1, Version 2.5.4

The above document and the specific portions of other documents referenced by it are the only documents that should be trusted to install, administer, or use the TOE in its evaluated configuration.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE consists of the Enveil ZeroReveal Compute Fabric Server v2.5.4 software when installed and configured in accordance with the documentation specified above in Section 6. The TOE has been evaluated on the following host platforms:

- CentOS 8.1 on Intel Core i7-10710U

Note: The TOE is the application software only. The host platforms are not part of the evaluation.

The TOE supports secure connectivity with several other IT environment devices as described below:

Component	Required	Usage/Purpose Description
Enveil ZeroReveal® Compute Fabric Server platform	Yes	The TOE is a ZeroReveal® Compute Fabric Server, which communicates with an instance of the ZeroReveal Client to process data queries in a way that does not disclose the nature of the query to any observer. The TOE does not serve a useful function without the ZeroReveal® Client. The Server platform must include the Java Runtime as shown in Figure 1 and the CentOS 8.1 OS as defined above.
Enveil ZeroReveal® Compute Fabric Client workstation	Yes	This is the client application which communicates with the ZeroReveal server to process data queries in a way that does not disclose the nature of the query to any observer. The workstation on which the Client runs must support the REST APIs used to communicate with the TOE.
Data Repository	Yes	Locally installed and configured databases containing information against which ZeroReveal queries are executed.

Table 6 IT Environment Components

7.2 Excluded Functionality

The TOE is a software application, and as such many of the functions of the application itself are out of scope of a Common Criteria Evaluation. The following functionality is explicitly excluded from the scope of evaluation; it was not evaluated during the common criteria evaluation, and no claims are made regarding the applicability, suitability, or functionality of the following TOE functions:

- Databases, including accessing, retrieving, storing, or operations on databases.
- The homomorphic encryption process, including the algorithms, uses and the security strength of the resultant ciphertext.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the Evaluation Test Report for Enveil ZeroReveal® Compute Fabric Server v2.5.4, which is not publicly available. The AAR provides an overview of testing and the prescribed AAs.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the PP_APP_v1.3 and PKG_TLS_V1.1. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here. A description of the test tools and test configurations may be found in Section 4 of the AAR.

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 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 Enveil ZeroReveal® Compute Fabric Server v2.5.4 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the AAs specified in the NDPP.

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 Enveil ZeroReveal® Compute Fabric Server v2.5.4 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the AAs specified in the PP_APP_v1.3 and PKG_TLS_V1.1.

The validator 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 EAL 1 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 (TSS). Additionally, the evaluator performed the AAs specified in the PP_APP_v1.3 and PKG_TLS_V1.1 related to the examination of the information contained in the TSS.

The validator 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 AAs, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 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 AAs specified in the PP_APP_v1.3 and PKG_TLS_V1.1 related to the examination of the information contained in the operational guidance documents.

The validator 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 AAs, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator 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 EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the AAs in the PP_APP_v1.3 and PKG_TLS_V1.1 and recorded the results in a Test Report, summarized in the ETR and AAR.

The validator 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 PP_APP_v1.3 and PKG_TLS_V1.1, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 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 potential vulnerabilities considered in the analysis is characterized by the date of the search (May 12, 2021), the search terms used, and the databases that were searched. This information is detailed in Section 7.5 of the AAR.

The validator 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 AAs in the PP_APP_v1.3 and PKG_TLS_V1.1, 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 AAs in the PP_APP_v1.3 and PKG_TLS_V1.1, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

All the validators' comments are covered in the Clarification of Scope section (5.3) of this report. There are no additional validator comments or recommendations.

11 Annexes

Not applicable.

12 Security Target

Enveil ZeroReveal® Compute Fabric Server Security Target Version 1.4.

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 VR:

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. Part 1: Introduction and general model.

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. Part 2: Security functional components.

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017. Part 3: Security assurance components.

[4] Common Methodology for Information Technology Security Evaluation, Version 3.1, 5, April 2017. Evaluation methodology.

[5] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[6] Enveil ZeroReveal® Compute Fabric Server v2.5.4 Security Target Version 1.4

[7] Enveil ZeroReveal® Compute Fabric Configuration Guide for Common Criteria v3.1, Version 2.5.4

[8] Assurance Activity Report for Enveil ZeroReveal® Compute Fabric Server v2.5.4 Version 1.3, May 28, 2021

[9] Evaluation Technical Report for Enveil ZeroReveal® Compute Fabric Server v2.5.4 Version 1.3, May 28, 2021

[10] Test Plan for Enveil ZeroReveal® Compute Fabric Server v2.5.4 Version 1.3, May 28, 2021