National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Enveil ZeroReveal™ Compute Fabric

Report Number: CCEVS-VR-VID10904-2018
Dated: August 28, 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

Table of Contents

1 Executive Summary 2
2 Identification 4
2.1 Threats 4
2.2 Assumptions..4
2.3 Organizational Security Policies..5
3 Architectural Information 6
4 Assumptions..7
4.1 Clarification of Scope 7
5 Security Policy 8
5.1 Cryptographic Support..8
5.2 User Data Protection 8
5.3 Identification and Authentication 8
5.4 Security Management 8
5.5 Privacy 8
5.6 Protection of the TSF..8
5.7 Trusted Path/Channels 8
6 Documentation..10
7 Independent Testing..11
7.1 Penetration Testing 13
8 Evaluated Configuration 14
9 Results of the Evaluation 15
10 Validator Comments/Recommendations 16
11 Annexes 17
12 Security Target..18
13 Abbreviations and Acronyms 19
14 Bibliography 20

List of Tables

Table 1: Evaluation Details 3
Table 2: ST and TOE Identification 4
Table 3 TOE Security Assurance Requirements 15

List of Figures

Figure 1 TOE Boundary 6
Figure 2 Test Configuration 12

1 Executive Summary

This report 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 Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should read carefully 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 Enveil ZeroReveal™ Compute Fabric. 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 of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the Enveil ZeroReveal™ Compute Fabric was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States, and was completed in July 2018. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in *Protection Profile for Application Software, Version 1.2, 22 April 2016*.

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that the Enveil ZeroReveal™ Compute Fabric is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) [7] and associated test report [6] produced by the Leidos evaluation team.

Enveil ZeroReveal™ Compute Fabric is an application consisting of the ZeroReveal Client Component and the ZeroReveal Server Component. The ZeroReveal Client Component resides within the enterprise and is responsible for encrypting ZeroReveal Compute Fabric operations and decrypting results. The ZeroReveal Server Component resides within the environment of a data repository and is responsible for processing encrypted operations over the data. Enveil ZeroReveal Compute Fabric enables data to remain encrypted even while being processed, thereby eliminating the risk of exposure. The Enveil ZeroReveal™ Compute Fabric also secures operations over unencrypted data by encrypting operations such as searches or analytics, and processing these encrypted operations over unencrypted data (without ever decrypting the operation), and produces encrypted results. Thus, a user is able to secure operations in untrusted environments such as data aggregators and data lakes in which they do not control the data or its encryption. The ZeroReveal Compute Fabric 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. In particular the TOE's homomorphic encryption and the associated encryption and decryption of searches and results are not part of the scope of this evaluation. The JDBC Driver library used to communicate with ZeroReveal Client instead of using the Client's REST API directly is also excluded. This evaluation makes no security claims about these features.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the 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.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	Enveil ZeroReveal™ Compute Fabric v1.1.1
Sponsor & Developer	Enveil 8171 Maple Lawn Blvd, Suite 240 Fulton, MD 20759
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	August 2018
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
PP	Protection Profile for Application Software, Version 1.2, 22 April 2016
Disclaimer	The information contained in this Validation Report is not an endorsement either expressed or implied of the Enveil ZeroReveal Compute Fabric.
Evaluation Personnel	Dawn Campbell Pascal Patin
Validation Personnel	Jerome Myers (Senior Validator) Jim Donndelinger (Senior Validator) Marybeth Panock (Lead Validator)

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) 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).

The following table identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	Enveil ZeroReveal™ Compute Fabric Security Target
ST Version	1.0
Publication Date	August 13, 2018
Vendor	Enveil
ST Author	Leidos
TOE Reference	Enveil ZeroReveal™ Compute Fabric
TOE Software Version	1.1.1
Keywords	Application

2.1 Threats

The ST references the *Protection Profile for Application Software, Version 1.2, 22 April 2016*. The protection profile identifies the following threats, which the TOE and its operational environment are intended to counter:

- 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.
- 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.
- 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.
- An attacker may try to access sensitive data at rest.

2.2 Assumptions

- The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.

- The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
- The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

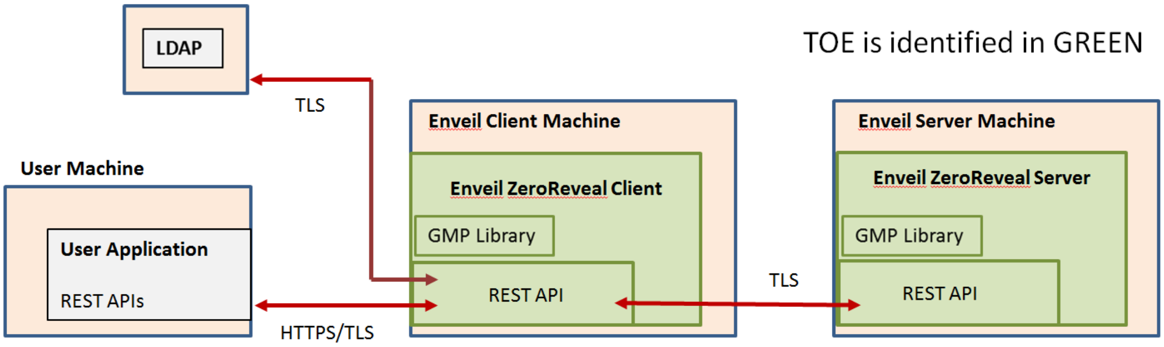
2.3 Organizational Security Policies

There are no Organizational Security Policies defined for the application in the PP.

3 Architectural Information

The section describes the TOE architecture including physical and logical boundaries. Figure 1 shows the TOE in relation to its operational environment.

Figure 1 TOE Boundary



The TOE consists of The Enveil ZeroReveal Compute Fabric and comprises the ZeroReveal Client Component and the ZeroReveal Server Component. The client's representational state transfer (REST) interfaces are within the scope of evaluation. The configuration files on each platform of the ZeroReveal Client and ZeroReveal Server Components are considered part of the TOE.

The TOE runs on Linux (CentOS 7.4 with SELinux) and the Java Runtime is the Oracle Java 8 JRE with the Unlimited Strength Jurisdiction Policy installed.

The ZeroReveal Client and ZeroReveal Server run on ordinary commodity hardware using general purpose x86_64 CPUs with at least 64 GB of available disk space.

The ZeroReveal Client and ZeroReveal Server rely on the Java Cryptographic Architecture for cryptographic services and on the GNU Multiple Precision Arithmetic Library (GMP) for arbitrary-precision arithmetic. The TOE is packaged with the GMP. The ZeroReveal Client Component and ZeroReveal Server Component rely on Linux tools (for example, Yum) in support of trusted update. The underlying operating system is Linux (CentOS 7.4 with SELinux) and the Java Runtime is the Oracle Java 8 JRE with the Unlimited Strength Jurisdiction Policy installed.

An external LDAP directory is required to authenticate users. Note that though Figure 1 depicts a single user machine, multiple user machines can connect to the ZR Client in the evaluated configuration.

4 Assumptions

The ST references the *Protection Profile for Application Software*, *Version 1.2*, *22 April 2016*, to identify following assumptions about the use of the product:

- The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
- The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
- The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

4.1 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:

1. 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 claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs and scoped to those Security Functional Requirements (SFRs) declared in the ST. Any additional security related functional capabilities of the product were not covered by this evaluation. In particular the TOE's homomorphic encryption and the associated encryption and decryption of searches and results are not part of the scope of this evaluation. The JDBC Driver library used to communicate with ZeroReveal Client instead of using the Client's REST API directly is also excluded.
4. 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.

5 Security Policy

The TOE enforces the following security policies as described in the ST.

5.1 Cryptographic Support

The TOE uses cryptographic services provided by the platform. Users communicate with ZeroReveal Client Component through REST interfaces protected by HTTPS/TLS. The ZeroReveal Client Component and ZeroReveal Server Component communicate via REST over mutually authenticated TLS. The ZeroReveal Client Component communicates with a LDAP Server using TLS. The TOE supports mutual authentication of the user connections at its REST interfaces; and with connections to the LDAP directory.

Credentials are stored in platform provided GNOME keyrings.

5.2 User Data Protection

The Enveil ZeroReveal Compute Fabric provides user data protection services by restricting access to only those platform-based resources (network communications) that are needed in order to provide the needed functionality.

The ZeroReveal Client initiates network communication to connect to the ZeroReveal Server and to the LDAP Server. The Client allows users to initiate a network connection through REST APIs.

5.3 Identification and Authentication

Enveil ZeroReveal Compute Fabric relies on certificate validation functions provided by the platform to authenticate the X.509 certificate as part of establishing a TLS connection.

5.4 Security Management

An enterprise manages the ZeroReveal Compute Fabric via configuration files stored in /etc as recommended by Linux.

5.5 Privacy

The ZeroReveal Client Component and ZeroReveal Server Component do not collect or transmit PII over a network.

5.6 Protection of the TSF

The ZeroReveal Compute Fabric uses Java APIs provided by the platform. The ZeroReveal Compute Fabric leverages platform provided package management for secure installation and updates. The TOE package includes only those third-party libraries necessary for its intended operation.   The TOE uses compiler provided anti-exploitation capabilities.

5.7 Trusted Path/Channels

The ZeroReveal Client and Server components are connected via mutually authenticated TLS over REST. The ZeroReveal Client Component communicates with an authentication server using Lightweight Directory Access Protocol (LDAP) secured with TLS. Users communicate with ZeroReveal Client

Component through REST. ZeroReveal Client Component requires HTTPS/TLS for connections to the REST interface.

6 Documentation

Enveil provides the following documents that provide information and guidance for the deployment of the TOE:

Enveil ZeroReveal Compute Fabric Configuration Guide for Common Criteria v3.1 Version 1.1.1, 2018

Enveil ZeroReveal Compute Fabric Manual Version 1.1.1, 2018

Note: the Enveil ZeroReveal Compute Fabric Configuration Guide for Common Criteria v3.1 document refers to specific sections of the Enveil ZeroReveal Compute Fabric Manual for configuring the TOE into the evaluated configuration. Only the Enveil ZeroReveal Compute Fabric Configuration Guide for Common Criteria v3.1 in conjunction with the referenced sections in the Enveil ZeroReveal Compute Fabric Manual should be used when configuring the TOE.

7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from the proprietary Test Report [6] as characterized in the following public document:

- Enveil ZeroReveal™ Compute Fabric Common Criteria Assurance Activities Report, version 1.0, 15 August 2018

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to the *Protection Profile for Application Software, Version 1.2, 22 April 2016*.

To this end, the evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the above-referenced Protection Profile.

The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report [6] and in the AAR listed above.

Testing of the TOE was performed from April 2, 2018 through April 6, 2018 at Enveil's offices in Fulton, Maryland.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory. For the purposes of testing, the configuration depicted in Figure 2 was used for testing the TOE. A single test computer was used to run test tools. It was also used for LDAP testing by running the OpenLDAP service on the Linux OS during those tests. OpenLDAP's built in TLS functionality was used to protect LDAP connections. Note that the IP address of the test computer sometimes changed during testing because of changes to the underlying network.

Testing involved the use of a single user client (the test computer) connecting to the ZeroReveal Client component, which in turn connected to the ZeroReveal Server component.

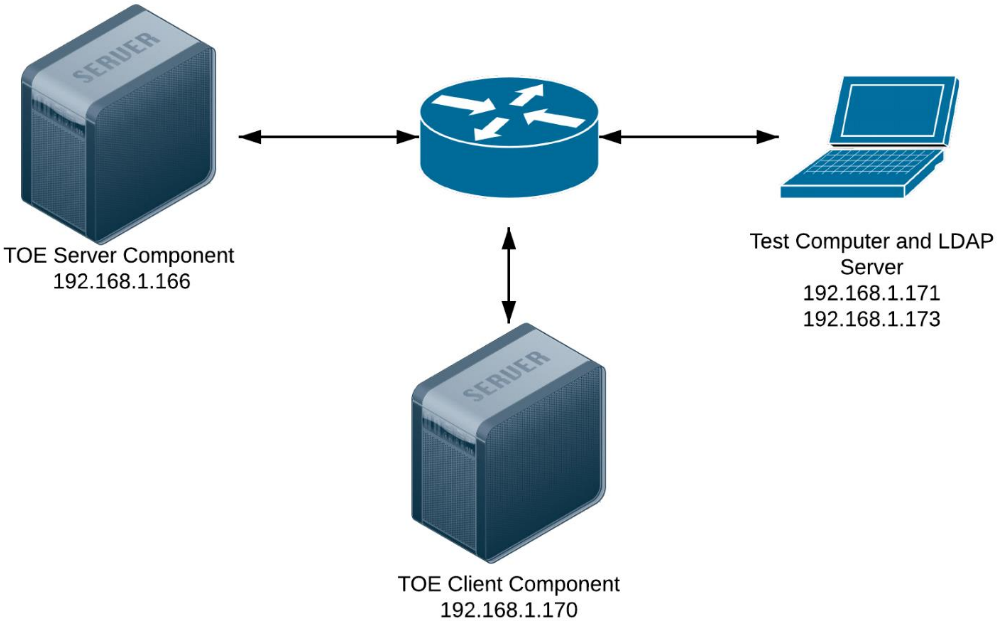


Figure 2 Test Configuration

As documented in the diagram above, the following hardware and software components were included in the evaluated configuration during testing:

TOE

- Enveil ZeroReveal Client Component
- Enveil ZeroReveal Server Component

Both TOE components were running on identical CentOS 7.4.1708 platforms. The platform hardware was an Intel NUC Kit 7i5BNH with the following specifications:

- Intel i5-7260U processor
- 8 GB of RAM
- 250GB SSD hard drive

Additional Components

- Linux Test Computer with Kali Linux 2018.1 rolling release, based on Linux kernel 4.14. The following programs and services were installed:
  - NIAP provided TLS test server tool, updated as of April 1, 2018
  - Leidos TLS test client tool, updated as of April 1, 2018
  - OpenSSL 1.1.0
  - XCA Certificate Authority 1.4.1
  - OpenLDAP 2.4.46
  - Wireshark 2.4.4

During testing the TOE was configured in standalone mode. As can be seen above, the configuration used during testing of the TOE matches that which was defined in the Security Target.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for the *Protection Profile for Application Software, Version 1.2, 22 April 2016* are fulfilled.

7.1 Penetration Testing

The evaluation team conducted an open-source search for vulnerabilities in the product. The open-source search did not identify any vulnerability applicable to the TOE in its evaluated configuration. Greater details on this search can be found in section 3.4.1 of the AAR. No additional testing was required to verify the vulnerabilities were mitigated.

8 Evaluated Configuration

The evaluated version of the TOE is Enveil ZeroReveal™ Compute Fabric v1.1.1. The TOE must be deployed as described in section 4 Assumptions of this document and must be configured in accordance with *Enveil ZeroReveal™ Compute Fabric Configuration Guide for Common Criteria Version 1.1.1*.

Per NIAP Publication #6 (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/scheme-pub-6.pdf), user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date. The product is still considered by NIAP to be in its evaluated configuration.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the *Protection Profile for Application Software, Version 1.2, 22 April 2016*.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 3 TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ASE_CCL.1	Conformance Claims
ASE_ECD.1	Extended Components Definition
ASE_INT.1	ST Introduction
ASE_OBJ.1	Security Objectives
ASE_REQ.1	Security Requirements
ASE_TSS.1	TOE Summary Specification
ADV_FSP.1	Basic Functional Specification
AGD_OPE.1	Operational User Guidance
AGD_PRE.1	Preparative Procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM Coverage
ALC_TSU_EXT.1	Timely Security Updates
ATE_IND.1	Independent Testing - Conformance
AVA_VAN.1	Vulnerability Survey

10 Validator Comments/Recommendations

The ‘Clarification of Scope’, section 4.1, explains what is not covered by this evaluation. The Validators’ only additional comment is to note that this evaluation needed a TRRT (576) to permit evaluation of the Enveil ZeroReveal^{TM} Compute Fabric as a distributed TOE against the Application Software Protection Profile v1.2. This was necessary because the App SW PP was not written to support distributed TOEs and the communications security functional requirements (SFRs) did not include those which are normally used to protect communication between the TOE components. TRRT 576 addressed this issue by specifying that network communication channels between TOE components are appropriately protected using SFRs that are supported by the App SW PP.

11 Annexes

Not applicable

12 Security Target

Name	Description
ST Title	Enveil ZeroReveal™ Compute Fabric Security Target
ST Version	Version 1.0
Publication Date	August 13, 2018

13 Abbreviations and Acronyms

API	Application programming interface
ASLR	Address space layout randomization
CC	Common Criteria
CLI	Command line interface
GMP	GNU Multiple Precision Arithmetic Library
GPG	GNU Privacy Guard
GUI	Graphical user interface
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IP	Internet Protocol
JAR	Java Archive
JDBC	Java Database Connectivity
JRE	Java Runtime Environment
LDAP	Lightweight Directory Access Protocol
NIAP	National Information Assurance Partnership
PII	Personally Identifiable Information
REST	Representational state transfer
RPM	RPM Package Manager
SAR	Security assurance requirement
SFR	Security functional requirement
TOE	Target of Evaluation
TLS	Transport Layer Security

14 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012.

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

[5] *Enveil ZeroReveal™ Compute Fabric Security Target*, Version 1.0, August 13, 2018

[6] *Enveil ZeroReveal™ Compute Fabric Common Criteria Test Report and Procedures*, Version 1.0, 15 August 2018

[7] *Enveil ZeroReveal™ Compute Fabric Common Criteria Assurance Activities Report*, Version 1.0, August 15, 2018

[8] *Enveil ZeroReveal™ Compute Fabric Configuration Guide for Common Criteria Version 1.1.1*, 2018

[9] *Evaluation Technical Report For Enveil ZeroReveal™ Compute Fabric*, Version 1.0 July 20, 2018