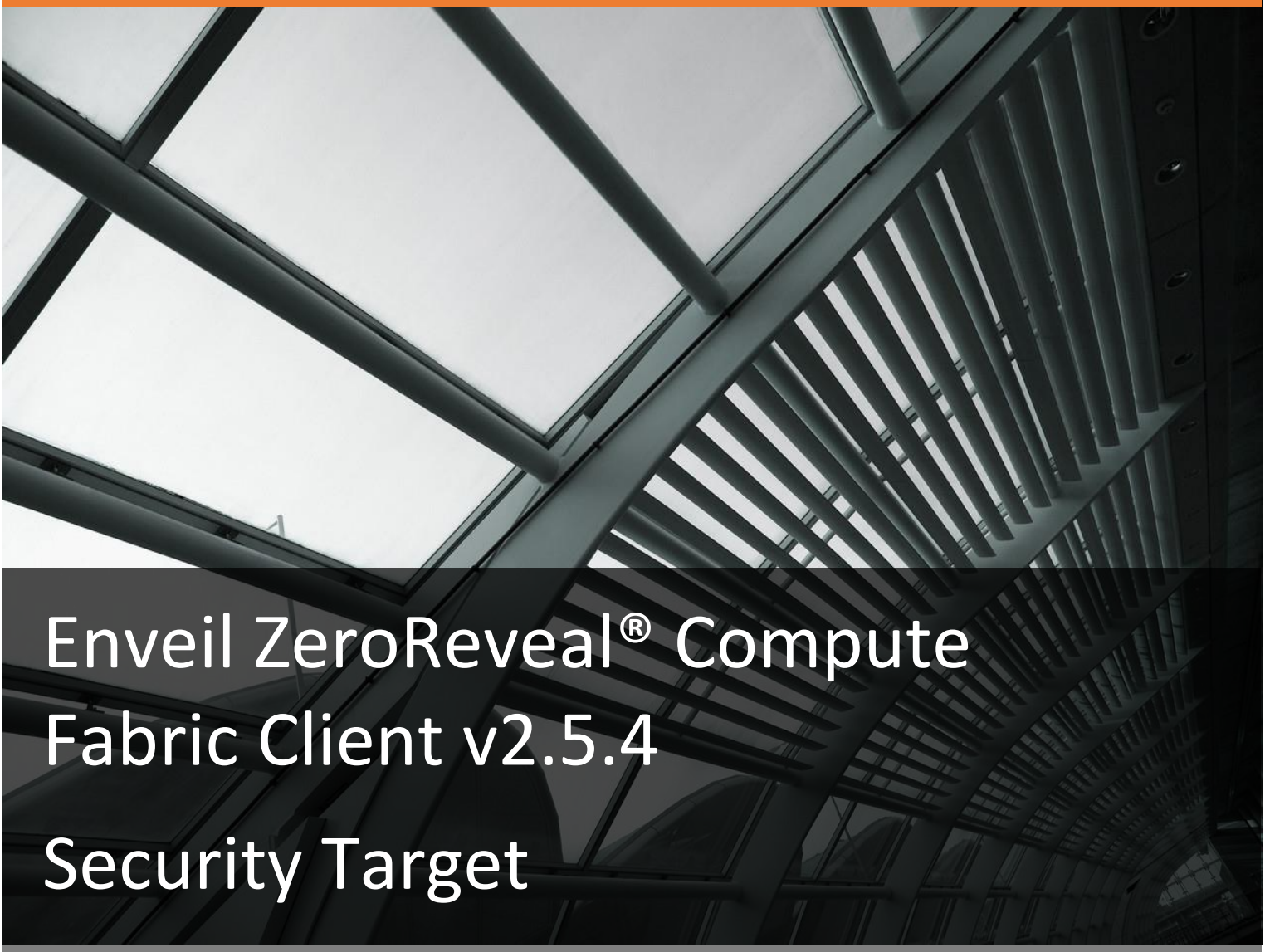

Enveil ZeroReveal® Compute Fabric Client v2.5.4

Security Target

Acumen Security, LLC.

Document Version: 1.4

Table Of Contents

Revision History

Version	Date	Description
0.1	2020-07-09	Initial Draft
0.2	2020-07-16	First Updates made
0.3	2020-07-24	Technical Decisions Implemented and HTTPS and TLS SFRs updated
0.4	2020-08-10	NIAP Check-in version
0.5	2020-11-23	Addressed validator comments
0.6	2021-03-08	Addressed evaluator comments
1.0	2021-05-10	Addressed validator check-out comments
1.1	2021-05-25	Addressed validator check-out comments
1.2	2021-05-26	Addressed validator check-out comments
1.3	2021-05-27	Addressed validator check-out comments
1.4	2021-06-01	Added TOE version to cover page

1 Security Target Introduction

1.1 Security Target and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

Category	Identifier
ST Title	Enveil ZeroReveal® Compute Fabric Client v2.5.4 Security Target
ST Version	1.4
ST Date	2021-06-01
ST Author	Acumen Security, LLC.
TOE Identifier	Enveil ZeroReveal® Compute Fabric Client v2.5.4
TOE Software Version	2.5.4
TOE Developer	Enveil
Key Words	Enveil, ZeroReveal, APP_PP, TLS_PKG

Table 1 TOE/ST Identification

1.2 TOE Overview

The Enveil ZeroReveal™ Compute Fabric enables data to remain encrypted even while being processed, thereby eliminating the risk of exposure. For example, a search against a dataset can be processed while keeping both the search and the contents of the dataset encrypted at all times. In addition to securing operations over encrypted data, the product also secures operations over unencrypted data. In this manner, the product encrypts operations such as searches or analytics, and processes 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 Client (the TOE) and ZeroReveal Server (evaluated separately) are evaluated as software applications only and the homomorphic encryption techniques used for the ZeroReveal Client and ZeroReveal Server operations are outside the scope of [PP APP SW].

Enveil's ZeroReveal™ Compute Fabric ecosystem consists of one ZeroReveal Client Component (the TOE) and one ZeroReveal Server Component (evaluated separately). 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. The ZeroReveal Compute Fabric encrypted data operations and the decrypting of the results are outside the scope of the [PP APP SW] and therefore not included in the evaluation.

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

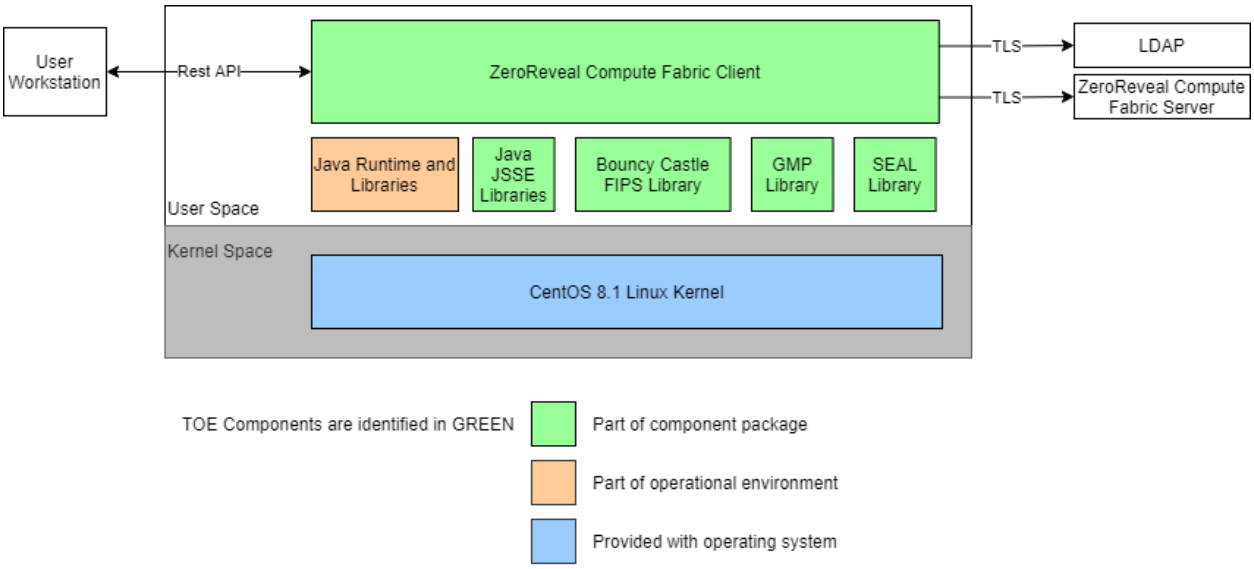

Figure 1 TOE Operational Environment

1.3 TOE Description

1.3.1 Evaluated Configuration

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 and required libraries 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	Yes	The TOE is a ZeroReveal® Compute Fabric Client, which communicates with a server 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® server.
Enveil ZeroReveal Compute Fabric Client platform	Yes	This is the platform on which the TOE is installed; 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 Client workstation must include the Java Runtime as shown in Figure 1 and the CentOS 8.1 OS as defined above.
LDAP Server	Yes	LDAP is used for external authentication and identification of users.
User Workstation	Yes	The TOE executes on a user workstation which must support the REST APIs used to communicate with the TOE.

Table 2 IT Environment Components

1.3.2 Physical Boundaries

The TOE is a software application and required libraries running on a host platform (as shown above).

1.3.3 Logical Boundaries

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

1.3.3.1 Cryptographic Support

The TOE performs two kinds of cryptographic functions: those necessary to the operation of the TOEs homomorphic encrypted search function, and those necessary to the operation of the trusted path and trusted channels. Because the homomorphic encryption functionality is outside the scope of this evaluation, only those cryptographic functions necessary to support the trusted path and trusted channels 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 3 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	FIPS Pub 180-4	Digest size 256 bits	C1874

Algorithm	Standard	Mode/Keysize	CAVP Cert. #
SHA2-384 SHA2-512		Digest size 384 bits Digest size 512 bits	
HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA-512	FIPS Pub 198-1	Key size 256 bits, block size 512 bits, digest size 256 bits Key size 384 bits, block size 1024 bits, digest size 384 bits Key size 512 bits, block size 1024 bits, digest size 512 bits	C1874

Table 4 CAVP Algorithm Testing References

1.3.3.2 User Data Protection

The ZeroReveal Client network communication is restricted to user-initiated communication for authentication via LDAP directory, responses to API requests, and initiation of communications with the ZeroReveal Server.

1.3.3.3 Identification and Authentication

The ZeroReveal client relies on X.509v3 certificate validation functions provided by the platform to authenticate the certificate(s) during the establishment of the TLS trusted channel. All trusted paths and channels are first authenticated using X.509v3 certificates.

Individual users are authenticated to the TOE by X.509v3 certificate during TLS with mutual authentication trusted channel establishment and by authentication via LDAP server (the first shows that the user is authorized to communicate with the TOE at all, the second shows that the user is authorized to run queries using the TOE).

1.3.3.4 Security Management

An enterprise administrator manages the TOE via configuration files on each installation workstation or platform in the Operational Environment. 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 configured credentials in the TOE's configuration files.

1.3.3.5 Privacy

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

1.3.3.6 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 utilizes compiler-provided anti-exploitation capabilities.

1.3.3.7 Trusted Path/Channels

The TOE communicates to the ZeroReveal® Compute Fabric Server via REST API over mutually authenticated TLS. The TOE communicates to the LDAP server via mutually authenticated TLS. Users communicate with the TOE through the REST API over HTTPS/TLS.

1.3.4 TOE Documentation

- Enveil ZeroReveal® Compute Fabric Client Security Target, v1.4, 2021-06-01 [ST]
- Enveil ZeroReveal® Compute Fabric Client Configuration Guide for Common Criteria v3.1, Version 2.5.4 [AGD]

1.3.5 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.

2 Conformance Claims

2.1 CC Conformance

This TOE is conformant to:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017: Part 2 extended
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017: Part 3 extended

2.2 Protection Profile Conformance

This TOE is conformant to:

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

2.3 Conformance Rationale

This Security Target provides exact conformance to Version 1.3 of the Protection Profile for Application Software and Version 1.1 of the Functional Package for Transport Layer Security (TLS). The security problem definition and security objectives in this Security Target are taken from the Protection Profile unmodified. The security requirements in this Security Target are all taken from the Protection Profile and Functional Package performing only operations defined there.

2.3.1 Technical Decisions

All NIAP Technical Decisions (TDs) issued to date that are applicable to [SWAPP] and [TLS-PKG] have been addressed. The following tables identify all applicable TD:

Identifier	Applicable	Exclusion Rationale (if applicable)
0588 – Session resumption support in TLS package	Yes	
0587 – X.509 SFR Applicability in App PP	Yes	
0582 – PP-Configuration for Application Software and Virtual Private Network (VPN) Clients now allowed	No	PP-configuration is not claimed for the toe
0561 – Signature verification update	Yes	
0554 – iOS/iPadOS/Android AppSW Virus Scan	No	The TOE is not an Android or iOS application
0548 – Integrity for installation tests in AppSW PP 1.3	No	The TOE is not an iOS application
0544 – Alternative testing methods for FPT_AEX_EXT.1.1	Yes	
0543 – FMT_MEC_EXT.1 evaluation activity update	No	The TOE is not a Windows application
0540 – Expanded AES Modes in FCS_COP	Yes	
0519 – Linux Symbolic Links and FMT_CFG_EXT.1	Yes	

Identifier	Applicable	Exclusion Rationale (if applicable)
0515 – Use Android APK Manifest in Test	No	The TOE is not an Android application
0513 – CA Certificate Loading	Yes	
0510 – Obtaining random bytes for iOS/macOS	No	The TOE is not an iOS/macOS application
0499 – Testing with Pinned certificates	No	The TOE does not support pinned certificates.
0498 – Application Software PP Security Objectives and Requirements Rationale	Yes	
0495 – FIA_X509_EXT.1.2 Test Clarification	Yes	
0473 – Support for Client or Server TOEs in FCS_HTTPS_EXT	Yes	
0469 – Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1	Yes	
0465 – Configuration Storage for .NET Apps	No	The TOE is not a .NET application
0445 – User Modifiable File Definition	Yes	
0442 – Updated TLS Ciphersuites for TLS Package	Yes	
0437 – Supported Configuration Mechanism	Yes	
0435 – Alternative to SELinux for FPT_AEX_EXT.1.3	Yes	
0434 – Windows Desktop Applications Test	No	This TD only applies to Windows platforms. The TOE runs on Linux.
0427 – Reliable Time Source	Yes	
0416 – Correction to FCS_RBG_EXT.1 Test Activity	Yes	

Table 5 Applicable Technical Decisions

3 Security Problem Definition

The security problem definition has been taken from [SWAPP] and is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any organizational security policies that the TOE is expected to enforce.

3.1 Threats

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 6 Threats

3.2 Assumptions

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 7 Assumptions

3.3 Organizational Security Policies

There are no OSPs for the application

[1] This Assumption is modified by TD0427.

4 Security Objectives

The security objectives have been taken from [SWAPP] and are reproduced here for the convenience of the reader.

4.1 Security Objectives for the TOE

The following security objectives for the TOE were drawn directly from the [SWAPP].

ID	TOE Objective
O.INTEGRITY	Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom, if ever, shipped without errors. The ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options. Addressed by: FDP_DEC_EXT.1, FMT_CFG_EXT.1, FPT_AEX_EXT.1, FPT_TUD_EXT.1
O.QUALITY	To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs. Addressed by: FMT_MEC_EXT.1, FPT_API_EXT.1, FPT_API_EXT.2, FPT_LIB_EXT.1, FPT_TUD_EXT.2, FCS_CKM.1(1)
O.MANAGEMENT	To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII. Addressed by: FMT_SMF.1, FPT_IDV_EXT.1, FPT_TUD_EXT.1, FPR_ANO_EXT.1, FCS_COP.1(3)
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data. Addressed by: FDP_DAR_EXT.1, FCS_STO_EXT.1, FCS_RBG_EXT.1, FCS_CKM.1(3), FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(4)
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application. Addressed by: FTP_DIT_EXT.1, FCS_RBG_EXT.1, FCS_RBG_EXT.2, FCS_CKM_EXT.1, FCS_CKM.2, FCS_HTTPS_EXT.1, FDP_NET_EXT.1, FIA_X509_EXT.1

Table 8 Objectives for the TOE

4.2 Security Objectives for the Operational Environment

The following security objectives for the operational environment assist the TOE in correctly providing its security functionality. These track with the assumptions about the environment.

ID	Objective for the Operation Environment
OE.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
OE.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.
OE.PROPER_ADMIN	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.

Table 9 Objectives for the environment

5 Security Requirements

This section identifies the Security Functional Requirements for the TOE and/or Platform. The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 and all international interpretations.

Requirement	Description
FCS_RBG_EXT.1	Random Bit Generation Services
FCS_RBG_EXT.2	Random Bit Generation from Application
FCS_CKM_EXT.1	Cryptographic Key Generation Services
FCS_CKM.1(1)	Cryptographic Asymmetric Key Generation
FCS_CKM.1(2)	Cryptographic Symmetric Key Generation
FCS_CKM.2	Cryptographic Key Establishment
FCS_COP.1(1)	Cryptographic Operation - Encryption/Decryption
FCS_COP.1(2)	Cryptographic Operation - Hashing
FCS_COP.1(3)	Cryptographic Operation - Signing
FCS_COP.1(4)	Cryptographic Operation - Keyed-Hash Message Authentication
FCS_HTTPS_EXT.1/Client	HTTPS Protocol for the Client
FCS_HTTPS_EXT.1/Server	HTTP Protocol for the Server
FCS_HTTPS_EXT.2	HTTPS Protocol with Mutual Authentication
FCS_STO_EXT.1	Storage of Credentials
FCS_TLS_EXT.1	TLS Protocol
FCS_TLSC_EXT.1	TLS Client Protocol
FCS_TLSC_EXT.2	TLS Client Support for Mutual Authentication
FCS_TLSC_EXT.3	TLS Client Support for Signature Algorithms Extension
FCS_TLSC_EXT.5	TLS Client Support for Supported Groups Extension
FCS_TLSS_EXT.1	TLS Server Protocol
FCS_TLSS_EXT.2	TLS Server Support for Mutual Authentication
FCS_TLSS_EXT.3	TLS Server Support for Signature Algorithms Extension
FDP_DEC_EXT.1	Access to Platform Resources
FDP_NET_EXT.1	Network Communications
FDP_DAR_EXT.1	Encryption Of Sensitive Application Data
FIA_X509_EXT.1	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FMT_MEC_EXT.1	Supported Configuration Mechanism
FMT_CFG_EXT.1	Secure by Default Configuration
FMT_SMF.1	Specification of Management Functions
FPR_ANO_EXT.1	User Consent for Transmission of Personally Identifiable Information
FPT_API_EXT.1	Use of Supported Services and APIs
FPT_AEX_EXT.1	Anti-Exploitation Capabilities

Requirement	Description
FPT_TUD_EXT.1	Integrity for Installation and Update
FPT_TUD_EXT.2	Integrity for Installation and Update
FPT_LIB_EXT.1	Use of Third Party Libraries
FPT_IDV_EXT.1	Software Identification and Versions
FTP_DIT_EXT.1	Protection of Data in Transit

Table 10 SFRs

5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with *italicized* text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3);
- Where operations were completed in the PP itself, the formatting used in the PP has been retained.

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs. Formatting conventions outside of operations matches the formatting specified within the PP.

5.2 Security Functional Requirements

5.2.1 Cryptographic Support (FCS)

FCS_RBG_EXT.1 Random Bit Generation Services

FCS_RBG_EXT.1.1

The application shall [*implement DRBG functionality*] for its cryptographic operations.

FCS_RBG_EXT.2 Random Bit Generation from Application

FCS_RBG_EXT.2.1

The application shall perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using [*HMAC_DRBG (any)*].

FCS_RBG_EXT.2.2

The deterministic RBG shall be seeded by an entropy source that accumulates entropy from a platform-based DRBG and [*no other noise source*] with a minimum of [*256 bits*] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

FCS_CKM_EXT.1 Cryptographic Key Generation Services

FCS_CKM_EXT.1.1

The application shall [*implement asymmetric key generation*].

FCS_CKM.1(1) Cryptographic Asymmetric Key Generation

FCS_CKM.1.1(1)

The application shall [*implement functionality*] **to generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm** [

- ***[ECC schemes]*** *using* ***["NIST curves" P-256, P-384 and [no other curves]]*** *that meet the following:* ***[FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4]*** *,*
- ***[RSA schemes]*** *using cryptographic key sizes of* ***[2048-bit or greater]*** *that meet the following* ***FIPS PUB 186-4, "Digital Signature Standard (DSS), Appendix B.3" ,***

].

FCS_CKM.1(2) Cryptographic Symmetric Key Generation

FCS_CKM.1.1(2)

The **application** shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1** and specified cryptographic key sizes [*256 bit*].

FCS_CKM.2 Cryptographic Key Establishment

FCS_CKM.2.1

The application shall [*implement functionality*] to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method:

[

- ***[Elliptic curve-based key establishment schemes]*** *that meets the following:* ***[NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"] ,***

].

FCS_COP.1(1) Cryptographic Operation - Encryption/Decryption[2]

FCS_COP.1.1(1)

The **application** shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm [

- *AES-CCM (as defined in NIST SP 800-38C) mode*
- *AES-GCM (as defined in NIST SP 800-38D) mode*

[2] This SFR has been modified by TD0540.

] and cryptographic key sizes [*256-bit*].

FCS_COP.1(2) Cryptographic Operation - Hashing

FCS_COP.1.1(2)

The **application** shall perform *cryptographic hashing* services in accordance with a specified cryptographic algorithm [

- *SHA-256,*
- *SHA-384,*
- *SHA-512,*

] and message digest sizes [

- *256,*
- *384,*
- *512,*

] bits that meet the following: FIPS Pub 180-4.

FCS_COP.1(3) Cryptographic Operation - Signing

FCS_COP.1.1(3)

The **application** shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [

- **RSA schemes** using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 4 ,
- ***ECDSA schemes*** *using "NIST curves" P-256, P-384 and [no other curves] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5*

] .

FCS_COP.1(4) Cryptographic Operation - Keyed-Hash Message Authentication

FCS_COP.1.1(4)

The **application** shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm HMAC-SHA-256 and [*SHA-384, SHA-512*] with key sizes [*256 bits, 384 bits, 512 bits*] and message digest sizes 256 and [*384, 512*] bits that meet the following: FIPS Pub 198-1 *The Keyed-Hash Message Authentication Code* and FIPS Pub 180-4 *Secure Hash Standard*.

FCS_HTTPS_EXT.1/Client HTTPS Protocol[3]

FCS_HTTPS_EXT.1.1/Client

The application shall implement the HTTPS protocol that complies with RFC 2818.

[3] This SFR has been modified by TD0473

FCS_HTTPS_EXT.1.2/Client

The application shall implement HTTPS using TLS as defined in the TLS package.

FCS_HTTPS_EXT.1.3/Client

The application shall [*not establish the application-initiated connection*] if the peer certificate is deemed invalid.

FCS_HTTPS_EXT.1/Server[4]

FCS_HTTPS_EXT.1.1/Server

The application shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2/Server

The application shall implement HTTPS using TLS as defined in the TLS package.

FCS_HTTPS_EXT.2 HTTPS Protocol with Mutual Authentication[5]

FCS_HTTPS_EXT.2.1

The application shall [*not establish the connection*] if the peer certificate is deemed invalid.

FCS_STO_EXT.1 Storage of Credentials

FCS_STO_EXT.1.1

The application shall [*implement functionality to securely store [LDAP X509 client certificates and private keys, TLS server and client certificates and private keys] according to [FCS_COP.1(1)*] to non-volatile memory.

FCS_TLS_EXT.1 TLS Protocol

FCS_TLS_EXT.1.1

The product shall implement [

- *TLS as a client,*
- *TLS as a server*

].

[4] This SFR was added by TD0473

[5] This SFR was added by TD0473

FCS_TLSC_EXT.1 TLS Client Protocol

FCS_TLSC_EXT.1.1[6]

The product shall implement TLS 1.2 (RFC 5246) and [*no earlier TLS versions*] as a client that supports the cipher suites [

- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*

] and also supports functionality for [*mutual authentication*].

FCS_TLSC_EXT.1.2

The product shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.3

The product shall not establish a trusted channel if the server certificate is invalid [*with no exceptions*].

FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

FCS_TLSC_EXT.2.1

The product shall support mutual authentication using X.509v3 certificates.

FCS_TLSC_EXT.3 TLS Client Support for Signature Algorithms Extension

FCS_TLSC_EXT.3.1

The product shall present the signature_algorithms extension in the Client Hello with the supported_signature_algorithms value containing the following hash algorithms: [*SHA256, SHA384*] and no other hash algorithms.

FCS_TLSC_EXT.5 TLS Client Support for Supported Groups Extension

FCS_TLSC_EXT.5.1

The product shall present the Supported Groups Extension in the Client Hello with the supported groups [

- *secp256r1,*
- *secp384r1*

].

[6] This SFR was modified by TD0442.

FCS_TLSS_EXT.1 TLS Server Protocol

FCS_TLSS_EXT.1.1[7]

The product shall implement TLS 1.2 (RFC 5246) and [*no earlier TLS versions*] as a server that supports the cipher suites [

- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*

] and no other cipher suites, and also supports functionality for [*mutual authentication, no session resumption or session tickets*].

FCS_TLSS_EXT.1.2

The product shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [*TLS 1.1*].

FCS_TLSS_EXT.1.3

The product shall perform key establishment for TLS using [*ECDHE parameters using elliptic curves [secp256r1, secp384r1] and no other curves*].

FCS_TLSS_EXT.2 TLS Server Support for Mutual Authentication

FCS_TLSS_EXT.2.1

The product shall support authentication of TLS clients using X.509v3 certificates.

FCS_TLSS_EXT.2.2

The product shall not establish a trusted channel if the client certificate is invalid.

FCS_TLSS_EXT.2.3

The product shall not establish a trusted channel if the Distinguished Name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match one of the expected identifiers for the client.

FCS_TLSS_EXT.3 TLS Server Support for Signature Algorithms Extension

FCS_TLSS_EXT.3.1

The product shall present the HashAlgorithm enumeration in supported_signature_algorithms in the Certificate Request with the following hash algorithms: [*SHA256, SHA384*] and no other hash algorithms.

5.2.2 User Data Protection (FDP)

FDP_DEC_EXT.1 Access to Platform Resources

FDP_DEC_EXT.1.1

The application shall restrict its access to [*network connectivity*].

[7] This SFR has been modified by TD0442 and TD0588

FDP_DEC_EXT.1.2

The application shall restrict its access to [*no sensitive information repositories*].

FDP_NET_EXT.1 Network Communications

FDP_NET_EXT.1.1

The application shall restrict network communication to [

- *user-initiated communication for [LDAP server, Enveil ZeroReveal® Compute Fabric Server],*
- *respond to [REST API requests from external clients],*
- *[LDAP Server, Enveil ZeroReveal® Compute Fabric Server]*

] .

FDP_DAR_EXT.1 Encryption Of Sensitive Application Data

FDP_DAR_EXT.1.1[8]

The application shall [

- *leverage platform-provided functionality to encrypt sensitive data*
- *protect sensitive data in accordance with FCS_STO_EXT.1,*

] in non-volatile memory.

5.2.3 Identification and Authentication (FIA)

FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1[9]

The application shall [*implement functionality*] to validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation
- The certificate path must terminate with a trusted CA certificate
- The application shall validate a certificate path by ensuring the presence of the basicConstraints extension, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met
- The application shall validate that any CA certificate includes caSigning purpose in the key usage field
- The application shall validate the revocation status of the certificate using [*CRL as specified in RFC 5280 Section 6.3*]
- The application shall validate the extendedKeyUsage (EKU) field according to the following rules:
    - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing Purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.

[8] This SFR has been modified by TD0486

[9] This SFR has been modified by TD0587.

- Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the EKU field.
- Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field.
- S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the EKU field.
- OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field.
- Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.

FIA_X509_EXT.1.2

The application shall treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 X.509 Certificate Authentication[10]

FIA_X509_EXT.2.1

The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [*HTTPS, TLS*].

FIA_X509_EXT.2.2

When the application cannot establish a connection to determine the validity of a certificate, the application shall [*not accept the certificate*].

5.2.4 Security Management (FMT)

FMT_MEC_EXT.1 Supported Configuration Mechanism[11]

FMT_MEC_EXT.1.1

The application shall [*invoke the mechanisms recommended by the platform vendor for storing and setting configuration options*].

FMT_CFG_EXT.1 Secure by Default Configuration

FMT_CFG_EXT.1.1

The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2

The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.

[10] This SFR has been modified by TD0587.
[11] This SFR has been modified by TD0437.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions [*no management functions*].

5.2.5 Privacy (FPR)

FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1

The application shall [*not transmit PII over a network]*.

5.2.6 Protection of TSF (FPT)

FPT_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1

The application shall use only documented platform APIs.

FPT_AEX_EXT.1 Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1

The application shall not request to map memory at an explicit address except for [*no exceptions*].

FPT_AEX_EXT.1.2

The application shall [*allocate memory regions with write and execute permissions for only [Coretto Java runtime performing just-in-time compilation]*].

FPT_AEX_EXT.1.3

The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4

The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5

The application shall be built with stack-based buffer overflow protection enabled.

FPT_TUD_EXT.1 Integrity for Installation and Update[12]

FPT_TUD_EXT.1.1

The application shall [*leverage the platform*] to check for updates and patches to the application

[12] This SFR has been modified by TD0561.

software.

FPT_TUD_EXT.1.2

The application shall **[***leverage the platform*] to query the current version of the application software.

FPT_TUD_EXT.1.3

The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4

Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5

The application is distributed [*as an additional software package to the platform OS*].

FPT_TUD_EXT.2 Integrity for Installation and Update[13]

FPT_TUD_EXT.2.1

The application shall be distributed using the format of the platform-supported package manager.

FPT_TUD_EXT.2.2

The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

FPT_TUD_EXT.2.3

The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.

FPT_LIB_EXT.1 Use of Third Party Libraries

FPT_LIB_EXT.1.1

The application shall be packaged with only [*SEAL homomorphic encryption Library, GNU Multiple Precision Arithmetic Library (GMP), Necessary Java dependencies*].

FPT_IDV_EXT.1 Software Identification and Versions

FPT_IDV_EXT.1.1

The application shall be versioned with [[*Version information in the log file*]].

[13] This SFR has been modified by TD0561.

5.2.7 Trusted Path/Channel (FTP)

FTP_DIT_EXT.1 Protection of Data in Transit[14]

FTP_DIT_EXT.1.1

The application shall [*encrypt all transmitted [data] with [HTTPS in accordance with FCS_HTTPS_EXT.1, TLS as defined in the TLS Package*] between itself and another trusted IT product.

5.3 TOE SFR Dependencies Rationale for SFRs

The Protection Profile for Application Software contains all the requirements claimed in this Security Target. As such, the dependencies are not applicable since the PP has been approved.

5.4 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the Protection Profile for Application Software which are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in the table below.

Assurance Class	Components	Components Description
Development	ADV_FSP.1	Basic functional specification
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
	ALC_TSU_EXT.1	Timely Security Updates
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_IND.1	Independent testing – conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

Table 11 Security Assurance Requirements

[14] This SFR has been modified by TD0587.

5.5 Rationale for Security Assurance Requirements

The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.

5.6 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by [Vendor] to satisfy the assurance requirements. The table below lists the details.

SAR	How the SAR will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated.
ALC_CMS.1	
ALC_TSU_EXT.1	Enveil uses a systematic method for identifying and providing security relevant updates to the TOEs users via its support infrastructure.
ATE_IND.1	Enveil will provide the TOE for testing.
AVA_VAN.1	Enveil will provide the TOE for testing.

Table 12 TOE Security Assurance Measures

6 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

SFR	Rationale
FCS_RBG_EXT.1 FCS_RBG_EXT.2	The TOE implements HMAC_DRBG Functionality to generate random bits for use in the rest of the cryptographic functions. The TOE utilizes a platform based DRBG as its noise source and seeds with a minimum of 256 bits of entropy. This is achieved using the SecuRandom Java class which is configured to use the /dev/random system device.
FCS_CKM_EXT.1 FCS_CKM.1(1) FCS_CKM.2 FCS_COP.1(3)	The TOE implements ECDSA Key Generation, Signature Generation, and Signature Verification as part of TLS trusted channel establishment. NIST curves P-256 and P-384 are supported. The implements RSA Key Generation, Signature Generation and Signature Verification as part of TLS trusted channel establishment. Key sizes of 2048-bits and greater are supported. Key establishment for TLS is performed using Elliptic Curve Diffie-Hellman with NIST curves P-256 and P-384.
FCS_CKM.1(2)	The TOE generates symmetric AES 256-bit keys for use in AES-GCM as part of TLS and for use in AES-CCM for protection of stored credentials.
FCS_COP.1(1)	The TOE performs encryption and decryption using AES-GCM for use in TLS trusted channels and using AES-CCM for use as part of protecting stored credentials.
FCS_COP.1(2) FCS_COP.1(4)	The TOE performs hashing and HMAC using: • SHA-256, using a 512-bit block size and 256-bit message digest size as part of digital signatures • SHA2-384, using a 1024-bit block size and 384-bit message digest size as part of TLS and digital signatures. • SHA2-512, using a 1024-bit block size and 512-bit message digest size as part of the authentication function used in key store and certificate formatting, and as the underlying DRBG function.
FCS_HTTPS_EXT.1/Client FCS_HTTPS_EXT.1/Server FCS_HTTPS_EXT.2	The TOE implements the HTTPS protocol according to RFC 2818 by implementing all SHALL, MUST, and SHOULD statements and by not implementing any SHALL NOT, MUST NOT, or SHOULD NOT statements. HTTPS is implemented using TLS 1.2 (RFC 5246). The TOE's REST interface does not accept a connection when a peer's certificate is invalid.
FCS_STO_EXT.1	The TOE implements secure storage of LDAP X.509v3 certificates (used for communicating with the LDAP server to authenticate users prior to use of the REST API), and TLS certificates and private keys (used as part of establishing

SFR	Rationale
	the TLS trusted channel with the Enveil ZeroReveal Server) by encrypting them with AES-CCM. The administrator configures a key, which is used in AES-CCM to decrypt the storage container.
FCS_TLS_EXT.1 FCS_TLSC_EXT.1 FCS_TLSC_EXT.2	The TOE acts as a TLS client when establishing connection to LDAP directory for authentication and when establishing connection to ZeroReveal Compute Fabric Server for operation requests and responses. When acting as a TLS client, the TOE supports mutual authentication using X.509v3 certificates. The TOE's certificate must contain the hostname or the IP address of the TOE's host machine as a Subject Alternative Name (SAN). The TOE validates the presented identifier in accordance with RFC 6125, and permits the reference identifier to be the CN, DN, or SAN-DNS. Where present, the SAN-DNS identifier supersedes the DN or CN values. Wildcards are supported, only in the leftmost label of the DNS identifier (ie, "*.example.server.com" but not "example.*.server.com"). The TOE does not support certificate pinning. When acting as a TLS client, the TOE implements TLSv1.2 and rejects all older TLS and SSL versions, and supports the following cipher suites: • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 The TOE supports Elliptic Curves Extension in the Client Hello with the secp256r1, and secp384r1 NIST curves. The supported curves are hardcoded and there are no configuration options. The TOE supports SHA256 and SHA384 signature hash algorithms after having configured the TOE according to the [AGD] The TOE performs X.509v3 certification validation. The TOE will reject trusted channel establishment if the certificate is invalid. The TOE implements mutual authentication for communication with the LDAP server and ZeroReveal Compute Fabric Server. The TOE uses X.509v3 certificates for identification and authentication of each endpoint.
FCS_TLSC_EXT.3	The TOE presents the signature_algorithm extension in the client_Hello message with a supported_signature_algorithms value containing only the SHA-256 and SHA-384 hash algorithms.
FCS_TLSC_EXT.5	The TOE implements the supported_Groups extension with groups secp256r1 and secp384r1 and no others.
FCS_TLS_EXT.1 FCS_TLSS_EXT.1	The TOE acts as a TLS server when accepting HTTPS connection requests from an end user.

SFR	Rationale
FCS_TLSS_EXT.2 FCS_TLSS_EXT.3	When acting as a TLS server, the TOE supports mutual authentication using X.509v3 certificates. The TOE validates the presented reference identifier in accordance with RFC 6125, and permits the reference identifier to be the CN, DN, or SAN-DNS. Where present, the SAN-DNS identifier supersedes the DN or CN values. When acting as a server, the TOE does not accept wildcards. When acting as a TLS server, the TOE performs ECDH key establishment using the secp256r1 or secp384r1 elliptic curves. The TOE does not support certificate pinning. When acting as a TLS server, the TOE implements TLSv1.2 and rejects all older versions of TLS and SSL, and supports the following cipher suites: • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 The TOE supports Elliptic Curves Extension in the Client Hello with the secp256r1, and secp384r1 NIST curves. The supported curves are hardcoded and there are no configuration options. The TOE supports SHA256 and SHA384 signature hash algorithms. The TOE performs X.509v3 certification validation. The TOE will reject trusted channel establishment if the certificate is invalid.
FDP_DEC_EXT.1	The TOE does not utilize any platform resources except network functionality. The TOE does not access sensitive information repositories. The guidance documentation identifies when the TOE requires network connectivity.
FDP_NET_EXT.1	The TOE permits the user to initiate communication to the LDAP server using TCP port 636 or 5636 or ZeroReveal Compute Fabric Server using TCP port 18443. The TOE responds to authenticated REST API requests over TCP port 17443.
FDP_DAR_EXT.1	The TOE protects application log files (stored in /var/log/enveil/client) using Linux filesystem encryption. The TOE implements secure storage of LDAP X.509v3 certificates, and TLS certificates and private keys (stored in /etc/enveil/client/certs) in accordance with FCS_STO_EXT.1.

SFR	Rationale
FIA_X509_EXT.1	The TOE uses X.509v3 certificates to authenticate network endpoints for the HTTPS/TLS trusted channel communications. The TOE complies with RFC 5280 by implementing all SHALL, SHOULD, and MUST statements and not implementing any SHALL NOT, SHOULD NOT, or MUST NOT statements. The TOE uses the Java PKIX and Bouncy Castle FIPS certificate validation tools. The notBefore and notAfter dates included in certificates will be checked to be before and after the current time respectively. Certificates received as part of TLS connections are checked for a valid path up to the certificate authority roots (which must have the X509v3 Basic Constraint CA: True). The TOE performs all of the required checks on trust path requirements, CA validity, key usages, and extended key usages. In the process, it ensures certificates presented for client authentication have the digitalSignature keyUsage and TLS Client extendedKeyUsage. CRL checking as specified in RFC 5280 Section 6.3 revocation checking will be attempted on certificates that have listed distribution points. It is a configuration option for administrators to decide if failure to determine a certificate's status (if that certificate lists an endpoint and the endpoint is unreachable) should result in certificate rejection. Enveil enables this platform-provided functionality by adding the java.security.cert.PKIXRevocationChecker class to the chain of X509 TrustManagers associated with TLS contexts used to form connections.
FIA_X509_EXT.2	The TOE uses X.509v3 certificates for TLS mutual authentication with REST API clients, and connections to the ZR Server and to LDAP servers. An administrator sets the certificate to be used for each distinct purpose in the TOE configuration file. When presented with an invalid certificate, the connections are rejected.
FMT_MEC_EXT.1	The TOE invokes the mechanisms recommended by the platform vendor for storing and setting configuration options. Global configuration options are stored in /etc/ and individual user configuration options are stored in /usr/local/enveil. Configuration files (modifiable by a text editor) are used to manage TOE configuration. Non-functional configuration file templates are put in place by the installer package. The components TOE stores configuration files in the /etc and home directories. The values and settings in the configuration files which are relevant to the Security Functional Requirements (SFRs) are identified below: • Configuration changes to Enveil property/configuration files can only be made by editing the configuration files with a text editor.
FMT_CFG_EXT.1	The TOE is not installed with default credentials.

SFR	Rationale
	The TOE installer package makes sure all configuration and data directories are configured with appropriate permissions to restrict against modification by unprivileged users. Once the TOE has been installed, the following configuration steps must be completed: • Set up TLS for the TOE. • Configure the TOE's LDAP interaction. • Assign the TOE client permissions in LDAP. • Configure at least one ZeroReveal Compute Fabric Server connection The TOE does not provide any functionality until an administrator provides configuration files.
FMT_SMF.1	An enterprise manages the TOE via configuration files on each platform. There is no management CLI, GUI, or interface to manage the TOE.
FPR_ANO_EXT.1	The TOE does not collect or transmit PII over a network.
FPT_API_EXT.1	Enveil only uses public APIs in the TOE. The TOE uses the following Linux APIs: java.beans.PropertyVetoException, java.io.BufferedInputStream, java.io.BufferedReader, java.io.BufferedWriter, java.io.ByteArrayInputStream, java.io.ByteArrayOutputStream, java.io.DataInputStream, java.io.DataOutputStream, java.io.EOFException, java.io.File, java.io.FileInputStream, java.io.FileNotFoundException, java.io.FileOutputStream, java.io.FileWriter, java.io.IOException, java.io.InputStream, java.io.InputStreamReader, java.io.ObjectInputStream, java.io.ObjectOutputStream, java.io.OutputStream, java.io.OutputStreamWriter, java.io.PipedInputStream, java.io.PipedOutputStream, java.io.PrintWriter, java.io.Reader, java.io.SequenceInputStream, java.io.Serializable, java.io.UncheckedIOException, java.io.Writer, java.lang.annotation.Annotation, java.lang.annotation.ElementType, java.lang.annotation.Inherited, java.lang.annotation.Repeatable, java.lang.annotation.Retention, java.lang.annotation.RetentionPolicy, java.lang.annotation.Target, java.lang.instrument.UnmodifiableClassException, java.lang.invoke.MethodHandle, java.lang.management.ManagementFactory, java.lang.ref.WeakReference, java.lang.reflect.Array, java.lang.reflect.Field, java.lang.reflect.InvocationTargetException, java.lang.reflect.Method, java.lang.reflect.ParameterizedType, java.lang.reflect.Proxy, java.lang.reflect.Type, java.math.BigDecimal, java.math.BigInteger,

SFR	Rationale
	java.net.ConnectException, java.net.InetAddress, java.net.MalformedURLException, java.net.Proxy, java.net.Socket, java.net.SocketException, java.net.URI, java.net.URISyntaxException, java.net.URL, java.net.UnknownHostException, java.nio.ByteBuffer, java.nio.charset.StandardCharsets, java.nio.file.DirectoryStream, java.nio.file.FileSystem, java.nio.file.FileSystems, java.nio.file.Files, java.nio.file.NoSuchFileException, java.nio.file.Path, java.nio.file.Paths, java.nio.file.StandardOpenOption, java.nio.file.attribute.PosixFilePermission, java.security.DigestInputStream, java.security.DigestOutputStream, java.security.InvalidAlgorithmParameterException, java.security.InvalidKeyException, java.security.InvalidParameterException, java.security.Key, java.security.KeyManagementException, java.security.KeyPair, java.security.KeyPairGenerator, java.security.KeyStore, java.security.KeyStoreException, java.security.MessageDigest, java.security.NoSuchAlgorithmException, java.security.NoSuchProviderException, java.security.Principal, java.security.Provider, java.security.PublicKey, java.security.SecureRandom, java.security.Security, java.security.SignatureException, java.security.UnrecoverableEntryException, java.security.UnrecoverableKeyException, java.security.cert.CertPathBuilder, java.security.cert.Certificate, java.security.cert.CertificateEncodingException, java.security.cert.CertificateException, java.security.cert.CertificateExpiredException, java.security.cert.CertificateFactory, java.security.cert.CertificateNotYetValidException, java.security.cert.CertificateParsingException, java.security.cert.PKIXBuilderParameters, java.security.cert.PKIXRevocationChecker, java.security.cert.X509CertSelector, java.security.cert.X509Certificate, java.security.interfaces.ECPrivateKey, java.security.interfaces.RSAPrivateCrtKey, java.security.interfaces.RSAPublicKey, java.security.spec.RSAKeyGenParameterSpec, java.sql.Connection, java.sql.Date, java.sql.DriverManager, java.sql.PreparedStatement, java.sql.ResultSet, java.sql.SQLException, java.sql.Statement, java.sql.Timestamp, java.sql.Types, java.text.DecimalFormat, java.text.Normalizer, java.text.NumberFormat, java.text.ParseException, java.text.SimpleDateFormat, java.time.Duration, java.time.Instant, java.time.LocalDate, java.time.LocalDateTime, java.time.ZoneOffset, java.time.format.DateTimeFormatter, java.util.AbstractList, java.util.AbstractMap, java.util.AbstractMap.SimpleEntry, java.util.ArrayList, java.util.Arrays, java.util.Base64, java.util.Calendar, java.util.Collection, java.util.Collections, java.util.Comparator, java.util.Date, java.util.Deque, java.util.EnumSet, java.util.Enumeration, java.util.HashMap, java.util.HashSet, java.util.Hashtable, java.util.Iterator, java.util.LinkedHashMap, java.util.LinkedHashSet, java.util.LinkedList,

SFR	Rationale
	java.util.List, java.util.Locale, java.util.Map, java.util.NoSuchElementException, java.util.Objects, java.util.Optional, java.util.OptionalInt, java.util.Properties, java.util.Queue, java.util.Random, java.util.ResourceBundle, java.util.Set, java.util.SortedSet, java.util.Spliterator, java.util.Spliterators, java.util.TimeZone, java.util.TimerTask, java.util.TreeMap, java.util.TreeSet, java.util.UUID, java.util.concurrent.AbstractExecutorService, java.util.concurrent.ArrayBlockingQueue, java.util.concurrent.BlockingQueue, java.util.concurrent.Callable, java.util.concurrent.CancellationException, java.util.concurrent.ConcurrentHashMap, java.util.concurrent.ConcurrentLinkedQueue, java.util.concurrent.ConcurrentMap, java.util.concurrent.CopyOnWriteArrayList, java.util.concurrent.CountDownLatch, java.util.concurrent.ExecutionException, java.util.concurrent.ExecutorService, java.util.concurrent.Executors, java.util.concurrent.Future, java.util.concurrent.ScheduledExecutorService, java.util.concurrent.ScheduledFuture, java.util.concurrent.Semaphore, java.util.concurrent.ThreadFactory, java.util.concurrent.ThreadLocalRandom, java.util.concurrent.TimeUnit, java.util.concurrent.TimeoutException, java.util.concurrent.atomic.AtomicBoolean, java.util.concurrent.atomic.AtomicInteger, java.util.concurrent.atomic.AtomicIntegerFieldUpdater, java.util.concurrent.atomic.AtomicLong, java.util.concurrent.atomic.AtomicReference, java.util.concurrent.locks.ReadWriteLock, java.util.concurrent.locks.ReentrantLock, java.util.concurrent.locks.ReentrantReadWriteLock, java.util.function.BiConsumer, java.util.function.BiPredicate, java.util.function.Consumer, java.util.function.DoubleConsumer, java.util.function.Function, java.util.function.Predicate, java.util.function.Supplier, java.util.logging.Level, java.util.logging.LogManager, java.util.logging.LogRecord, java.util.logging.Logger, java.util.regex.Matcher, java.util.regex.Pattern, java.util.stream.Collectors, java.util.stream.IntStream, java.util.stream.Stream, java.util.stream.StreamSupport, java.util.zip.GZIPInputStream, java.util.zip.GZIPOutputStream, javax.annotation.Generated, javax.annotation.processing.AbstractProcessor, javax.annotation.processing.RoundEnvironment, javax.annotation.processing.SupportedAnnotationTypes, javax.annotation.processing.SupportedSourceVersion, javax.crypto.BadPaddingException, javax.crypto.Cipher, javax.crypto.IllegalBlockSizeException, javax.crypto.KeyGenerator, javax.crypto.NoSuchPaddingException, javax.crypto.SealedObject, javax.crypto.SecretKey, javax.crypto.SecretKeyFactory,

SFR	Rationale
	javax.crypto.spec.IvParameterSpec, javax.crypto.spec.SecretKeySpec, javax.inject.Inject, javax.inject.Provider, javax.inject.Singleton, javax.jms.ConnectionFactory, javax.lang.model.SourceVersion, javax.lang.model.element.Element, javax.lang.model.element.ElementKind, javax.lang.model.element.TypeElement, javax.management.MBeanServer, javax.naming.AuthenticationNotSupportedException, javax.naming.CommunicationException, javax.naming.NamingEnumeration, javax.naming.NamingException, javax.naming.directory.Attribute, javax.naming.directory.SearchControls, javax.naming.directory.SearchResult, javax.naming.ldap.LdapContext, javax.net.SocketFactory, javax.net.ssl.CertPathTrustManagerParameters, javax.net.ssl.KeyManager, javax.net.ssl.KeyManagerFactory, javax.net.ssl.SSLContext, javax.net.ssl.SSLEngine, javax.net.ssl.SSLException, javax.net.ssl.SSLHandshakeException, javax.net.ssl.SSLServerSocket, javax.net.ssl.SSLSession, javax.net.ssl.SSLSessionContext, javax.net.ssl.SSLSocket, javax.net.ssl.SSLSocketFactory, javax.net.ssl.TrustManager, javax.net.ssl.TrustManagerFactory, javax.net.ssl.X509TrustManager, javax.persistence.Access, javax.persistence.AccessType, javax.persistence.CascadeType, javax.persistence.Column, javax.persistence.DiscriminatorColumn, javax.persistence.DiscriminatorValue, javax.persistence.ElementCollection, javax.persistence.Embeddable, javax.persistence.Embedded, javax.persistence.EmbeddedId, javax.persistence.Entity, javax.persistence.EnumType, javax.persistence.Enumerated, javax.persistence.FetchType, javax.persistence.GeneratedValue, javax.persistence.Id, javax.persistence.Index, javax.persistence.Inheritance, javax.persistence.InheritanceType, javax.persistence.JoinColumn, javax.persistence.JoinTable, javax.persistence.Lob, javax.persistence.ManyToMany, javax.persistence.ManyToOne, javax.persistence.OneToMany, javax.persistence.OneToOne, javax.persistence.Query, javax.persistence.Table, javax.persistence.Temporal, javax.persistence.TemporalType, javax.persistence.Transient, javax.persistence.TypedQuery, javax.persistence.criteria.CriteriaBuilder, javax.persistence.criteria.CriteriaQuery, javax.persistence.criteria.Expression, javax.persistence.criteria.Predicate, javax.persistence.criteria.Root, javax.persistence.criteria.Selection, javax.persistence.criteria.SetJoin, javax.security.auth.login.Configuration, javax.security.auth.x500.X500Principal, javax.servlet.http.HttpServletRequest, javax.sql.DataSource, javax.tools.Diagnostic, javax.tools.FileObject, javax.tools.StandardLocation, javax.validation.ValidationException, javax.validation.constraints.Min, javax.validation.constraints.NotNull, javax.validation.constraints.Size, javax.ws.rs.Consumes, javax.ws.rs.DELETE, javax.ws.rs.DefaultValue, javax.ws.rs.ForbiddenException, javax.ws.rs.GET, javax.ws.rs.InternalServerErrorException, javax.ws.rs.NotAllowedException,

SFR	Rationale
	javax.ws.rs.NotFoundException, javax.ws.rs.PATCH, javax.ws.rs.POST, javax.ws.rs.PUT, javax.ws.rs.Path, javax.ws.rs.PathParam, javax.ws.rs.ProcessingException, javax.ws.rs.Produces, javax.ws.rs.QueryParam, javax.ws.rs.WebApplicationException, javax.ws.rs.client.Client, javax.ws.rs.client.WebTarget, javax.ws.rs.container.ContainerRequestContext, javax.ws.rs.container.ContainerRequestFilter, javax.ws.rs.container.ContainerResponseContext, javax.ws.rs.container.ContainerResponseFilter, javax.ws.rs.container.PreMatching, javax.ws.rs.core.Context, javax.ws.rs.core.Cookie, javax.ws.rs.core.Feature, javax.ws.rs.core.FeatureContext, javax.ws.rs.core.HttpHeaders, javax.ws.rs.core.MediaType, javax.ws.rs.core.MultivaluedMap, javax.ws.rs.core.NewCookie, javax.ws.rs.core.Request, javax.ws.rs.core.Response, javax.ws.rs.core.Response.Status, javax.ws.rs.core.SecurityContext, javax.ws.rs.core.StreamingOutputjavax.ws.rs.core.UriBuilder, javax.ws.rs.core.UriInfo, javax.ws.rs.ext.ExceptionMapper, javax.ws.rs.ext.MessageBodyReader, javax.ws.rs.ext.MessageBodyWriter, javax.ws.rs.ext.ParamConverter, javax.ws.rs.ext.ParamConverterProvider, javax.ws.rs.ext.Provider, javax.ws.rs.ext.Providers, javax.xml.XMLConstants, javax.xml.bind.DatatypeConverter, javax.xml.parsers.DocumentBuilder, javax.xml.parsers.DocumentBuilderFactory, javax.xml.parsers.ParserConfigurationException, javax.xml.transform.Source, javax.xml.transform.dom.DOMSource, javax.xml.transform.stream.StreamSource, javax.xml.validation.Schema, javax.xml.validation.SchemaFactory, javax.xml.validation.Validator, sun.security.x509.X500Name, The included GMP library imports these C/C++ headers: Algorithm, assert.h, cfloat, cstring, ctype.h, errno.h, , fcntl.h, float.h, gmp.h, ia64intrin.h, intrinsics.h, inttypes.h, invent.h, iosfwd, langinfo.h, limits, limits.h, locale.h, machine/builtins.h, machine/hal_sysinfo.h, math.h, nl_types.h, obstack.h, readline/history.h, readline/readline.h, setjmp.h, signal.h, sstream, stdarg.h, stddef.h, stdexcept, stdint.h, stdio.h, stdlib.h, string, string.h, strstream, sys/attributes.h, sys/ioctl.h, sys/iograph.h, sys/mman.h, sys/param.h, sys/processor.h, sys/pstat.h, sys/resource.h, sys/sysctl.h, sys/sysinfo.h, sys/syssgi.h, sys/systemcfg.h, sys/time.h, sys/times.h, sys/types.h, time.h, type_traits, unistd.h, utility The included SEAL library imports these C/C++ headers: Algorithm, array, atomic, cmath, complex, cstddef, cstdint, cstring, exceptions.h, functional, gsl/gsl, intrin.h, iostream, jni.h, limits, map, memory, mutex, new, numeric, random, shared_mutex, sstream, stdexcept, stdio.h, string, thread, tuple, type_traits, unordered_map, utility, vector, wmmintrin.h, x86intrin.h

SFR	Rationale
FPT_AEX_EXT.1	The main TOE application code is written in Java which places calls out to native C/C++ binaries. The Java binaries rely on the JRE for memory and stack protection, which are compiled into the JRE used in the OE by the JRE vendor. The two native code libraries in the TOE: SEAL and GMP. GMP and SEAL are compiled using GCC with the required compiler flags for ASLR (GCC CFLAG –fPIC, "Generate position-independent code") and stack protection (-fstackprotector-all). The memory protections for the GMP and SEAL native code portion were verified through static analysis. The TOE allocates memory regions with write and execute permissions for Coretto OpenJDK Java runtime performing just-in-time compilation. The TOE installs data and library files to /usr/local/enveil/* and configuration files to /etc/enveil/*. By default, the installed directories containing user-modifiable files do not have executables in them.
FPT_TUD_EXT.1 FPT_TUD_EXT.2	Enveil will publish Yum repositories for updates and patches to the TOE. The TOE relies on Yum to periodically poll the repositories for updates and notify the user. The TOE does not check for or apply updates on its own. The TOE relies on the platform to secure communication with the Enveil repositories. If Enveil's repository server is not accessible over the network from the location of the TOE (for example, if the TOE has been installed on a machine without internet access), the enterprise will need to mirror the repositories locally. The TOE supports packages running on Red Hat and Red Hat derivatives in RPM format. Official Enveil RPMs are signed using Enveil's private signing key. When using yum to install Enveil TOE packages, the GPG signatures on the RPM files will automatically be checked. If they are missing a signature or signed with the wrong GPG key, then an error indicating that the GPG keys for the repository do not match the package will be displayed and the install will automatically abort. These checks are also run during the installation of every update. The TOE records its version in the RPM package file. An administrator can determine the current version by running the command `yum info enveil-client`. The update/install packages include the required information so that the package manager will perform removal and deletion of all traces of the application when an uninstall command is issued through that package manager. The TOE is updated using the platform package manager. When Enveil developers finish a new version of any component, they sign then upload it to the package repositories, which make it available to users. Updates are

SFR	Rationale
	initiated by users via the package manager; the TOE will never download, modify, replace or update its own binary code. Enveil provides a changelog as part of the documentation accompanying every update. This changelog communicates any changes to security properties or configuration that occurred as part of the update. Enveil provides a public-facing e-mail address (bugs@enveil.com) that users can use to report security vulnerabilities involving any part of the TOE. This address is communicated to users in the ZeroReveal Platform guide and the Enveil website. A public PGP key is provided on the website at https://enveil.com/bugs, which can be used to encrypt reports sent to this e-mail.
FPT_LIB_EXT.1	The TOE is packaged with the SEAL Homomorphic Encryption Library and the GNU Multiple Precision Arithmetic Library, and those java dependencies required for the JRE to execute. No other third-party libraries are included with the TOE. The Java / Maven dependencies are listed below: javax.activation:activation:1.1.1 org.apache.activemq:activemq-all:5.16.1 org.sonatype.aether:aether-api:1.13.1 org.sonatype.aether:aether-connector-asynchttpclient:1.13.1 org.sonatype.aether:aether-connector-file:1.13.1 org.sonatype.aether:aether-impl:1.13.1 org.sonatype.aether:aether-spi:1.13.1 org.sonatype.aether:aether-util:1.13.1 io.airlift:aircompressor:0.13 org.jetbrains:annotations:13.0 com.google.code.findbugs:annotations:3.0.1u2 antlr:antlr:2.7.7 org.antlr:antlr4-runtime:4.9.1 aopalliance:aopalliance:1.0 org.glassfish.hk2.external:aopalliance-repackaged:2.5.0-b62 log4j:apache-log4j-extras:1.2.17 org.ow2.asm:asm:9.1 org.ow2.asm:asm-analysis:6.2.1 org.ow2.asm:asm-tree:6.2.1 org.ow2.asm:asm-util:6.2.1 com.ning:async-http-client:1.6.5 com.google.auto.value:auto-value-annotations:1.7.4 org.bouncycastle:bc-fips:1.0.2 org.bouncycastle:bctls-fips:1.0.10 io.airlift:bootstrap:202 org.apache.bval:bval-core:1.1.2 org.apache.bval:bval-jsr:1.1.2 net.bytebuddy:byte-buddy:1.10.17

SFR	Rationale
	io.airlift:bytecode:1.1 com.mchange:c3p0:0.9.5.5 cglib:cglib-nodep:3.3.0 org.checkerframework:checker-qual:3.5.0 com.fasterxml:classmate:1.5.1 commons-beanutils:commons-beanutils:1.9.4 commons-codec:commons-codec:1.15 commons-collections:commons-collections:3.2.2 commons-io:commons-io:2.8.0 org.apache.commons:commons-lang3:3.11 commons-logging:commons-logging:1.2 org.apache.commons:commons-math3:3.6.1 commons-pool:commons-pool:1.5.4 org.apache.commons:commons-text:1.6 io.airlift:concurrent:202 com.typesafe:config:1.4.1 io.airlift:configuration:202 org.conscrypt:conscrypt-openjdk-uber:2.4.0 io.airlift:discovery:0.178 io.airlift.discovery:discovery-server:1.29 org.dom4j:dom4j:2.1.3 net.sf.ehcache:ehcache-core:2.6.11 org.ejml:ejml-core:0.34 org.ejml:ejml-ddense:0.34 com.google.errorprone:error_prone_annotations:2.3.4 com.esri.geometry:esri-geometry-api:2.2.4 io.airlift:event:0.178 net.jodah:failsafe:2.0.1 com.google.guava:failureaccess:1.0.1 com.sun.xml.fastinfoset:FastInfoset:1.2.15 it.unimi.dsi:fastutil:8.5.2 net.sf.geographiclib:GeographicLib-Java:1.49 ch.hsr:geohash:1.4.0 org.glassfish.grizzly:grizzly-framework:2.4.4 org.glassfish.grizzly:grizzly-http:2.4.4 org.glassfish.grizzly:grizzly-http-server:2.4.4 org.glassfish.grizzly:grizzly-http-servlet:2.4.4 org.glassfish.grizzly:grizzly-portunif:2.4.4 org.glassfish.grizzly:grizzly-websockets:2.4.4 com.google.code.gson:gson:2.8.6 org.geotools:gt-main:24.2 org.geotools:gt-metadata:24.2 org.geotools:gt-opengis:24.2 org.geotools:gt-referencing:24.2 com.google.guava:guava:30.1-jre com.google.inject:guice:4.2.3

SFR	Rationale
	com.google.inject.extensions:guice-assistedinject:4.2.3 org.glassfish.hk2:guice-bridge:2.5.0-b62 com.google.inject.extensions:guice-multibindings:4.2.3 com.h2database:h2:1.4.197 org.hdrhistogram:HdrHistogram:2.1.9 org.hibernate:hibernate-c3p0:5.4.28.Final org.hibernate.common:hibernate-commons-annotations:5.1.2.Final org.hibernate:hibernate-core:5.4.28.Final org.glassfish.hk2:hk2-api:2.5.0-b62 org.glassfish.hk2:hk2-locator:2.5.0-b62 org.glassfish.hk2:hk2-utils:2.5.0-b62 io.airlift:http-client:202 io.airlift:http-server:0.178 org.eclipse.jetty.http2:http2-client:9.4.30.v20200611 org.eclipse.jetty.http2:http2-common:9.4.14.v20181114 org.eclipse.jetty.http2:http2-hpack:9.4.14.v20181114 org.eclipse.jetty.http2:http2-http-client-transport:9.4.30.v20200611 org.eclipse.jetty.http2:http2-server:9.4.14.v20181114 tech.units:indriya:2.0.2 com.sun.istack:istack-commons-runtime:3.0.7 com.google.j2objc:j2objc-annotations:1.3 com.fasterxml.jackson.core:jackson-annotations:2.12.1 com.fasterxml.jackson.core:jackson-core:2.12.1 com.fasterxml.jackson.core:jackson-databind:2.12.1 com.fasterxml.jackson.dataformat:jackson-dataformat-smile:2.9.7 com.fasterxml.jackson.dataformat:jackson-dataformat-yaml:2.11.1 com.fasterxml.jackson.datatype:jackson-datatype-guava:2.10.3 com.fasterxml.jackson.datatype:jackson-datatype-jdk8:2.10.3 com.fasterxml.jackson.datatype:jackson-datatype-joda:2.12.1 com.fasterxml.jackson.datatype:jackson-datatype-jsr310:2.10.3 com.fasterxml.jackson.jaxrs:jackson-jaxrs-base:2.12.1 com.fasterxml.jackson.jaxrs:jackson-jaxrs-json-provider:2.12.1 com.fasterxml.jackson.module:jackson-module-jaxb-annotations:2.12.1 com.fasterxml.jackson.module:jackson-module-parameter-names:2.10.3 javax.media:jai_core:1.1.3 com.sun.activation:jakarta.activation:2.0.0 jakarta.activation:jakarta.activation-api:1.2.1 jakarta.annotation:jakarta.annotation-api:1.3.4 org.glassfish.hk2.external:jakarta.inject:2.5.0 jakarta.ws.rs:jakarta.ws.rs-api:2.1.5 jakarta.xml.bind:jakarta.xml.bind-api:3.0.0 org.jboss:jandex:2.2.3.Final com.github.zafarkhaja:java-semver:0.9.0 org.javassist:javassist:3.27.0-GA javax.activation:javax.activation-api:1.2.0 javax.annotation:javax.annotation-api:1.3.2

SFR	Rationale
	javax.inject:javax.inject:1 org.glassfish.hk2.external:javax.inject:2.5.0-b62 javax.persistence:javax.persistence-api:2.2 javax.servlet:javax.servlet-api:4.0.1 javax.ws.rs:javax.ws.rs-api:2.1.1 javax.xml.bind:jaxb-api:2.3.1 org.glassfish.jaxb:jaxb-runtime:2.3.1 io.airlift:jaxrs:0.178 org.jboss.logging:jboss-logging:3.4.1.Final org.jboss.spec.javax.transaction:jboss-transaction-api_1.2_spec:1.1.1.Final net.jcip:jcip-annotations:1.0 org.slf4j:jcl-over-slf4j:1.7.16 org.glassfish.jersey.core:jersey-client:2.28 org.glassfish.jersey.core:jersey-common:2.28 org.glassfish.jersey.containers:jersey-container-grizzly2-http:2.28 org.glassfish.jersey.containers:jersey-container-servlet:2.22.2 org.glassfish.jersey.containers:jersey-container-servlet-core:2.28 org.glassfish.jersey.inject:jersey-hk2:2.28 org.glassfish.jersey.media:jersey-media-jaxb:2.28 org.glassfish.jersey.media:jersey-media-multipart:2.28 org.glassfish.jersey.core:jersey-server:2.28 org.eclipse.jetty:jetty-alpn-client:9.4.30.v20200611 org.eclipse.jetty:jetty-alpn-openjdk8-client:9.4.30.v20200611 org.eclipse.jetty:jetty-client:9.4.30.v20200611 org.eclipse.jetty:jetty-http:9.4.14.v20181114 org.eclipse.jetty:jetty-io:9.4.14.v20181114 org.eclipse.jetty:jetty-jmx:9.4.14.v20181114 org.eclipse.jetty:jetty-security:9.4.14.v20181114 org.eclipse.jetty:jetty-server:9.4.14.v20181114 org.eclipse.jetty:jetty-servlet:9.4.14.v20181114 org.eclipse.jetty:jetty-util:9.4.14.v20181114 org.jgrapht:jgrapht-core:0.9.0 it.geosolutions.jgridshift:jgridshift-core:1.3 io.jsonwebtoken:jjwt:0.9.0 io.airlift:jmx:0.178 io.airlift:jmx-http:0.178 io.airlift:jmx-http-rpc:0.159 org.weakref:jmxutils:1.21 net.java.dev.jna:jna:5.7.0 joda-time:joda-time:2.10.6 io.airlift:joda-to-java-time-bridge:3 org.openjdk.jol:jol-core:0.2 io.airlift:joni:2.1.5.1 io.airlift:json:202 com.jayway.jsonpath:json-path:2.5.0 com.google.code.findbugs:jsr305:3.0.2

SFR	Rationale
	org.locationtech.jts:jts-core:1.18.1 org.slf4j:jul-to-slf4j:1.7.30 org.jetbrains.kotlin:kotlin-stdlib:1.4.20 org.jetbrains.kotlin:kotlin-stdlib-common:1.4.20 org.iq80.leveldb:leveldb:0.10 org.iq80.leveldb:leveldb-api:0.10 com.google.guava:listenablefuture:9999.0-empty-to-avoid-conflict-with-guava io.airlift:log:0.178 io.airlift:log-manager:0.178 log4j:log4j:1.2.17 ch.qos.logback:logback-core:1.2.3 org.apache.lucene:lucene-analyzers-common:8.8.1 org.apache.lucene:lucene-core:8.8.1 org.apache.lucene:lucene-memory:8.8.1 org.apache.lucene:lucene-queries:8.8.1 org.apache.lucene:lucene-queryparser:8.8.1 org.apache.lucene:lucene-sandbox:8.8.1 org.lz4:lz4-java:1.7.1 org.apache.maven:maven-aether-provider:3.0.4 org.apache.maven:maven-artifact:3.0.4 org.apache.maven:maven-compat:3.0.4 org.apache.maven:maven-core:3.0.4 org.apache.maven:maven-embedder:3.0.4 org.apache.maven:maven-model:3.0.4 org.apache.maven:maven-model-builder:3.0.4 org.apache.maven:maven-plugin-api:3.0.4 org.apache.maven:maven-repository-metadata:3.0.4 org.apache.maven:maven-settings:3.0.4 org.apache.maven:maven-settings-builder:3.0.4 com.mchange:mchange-commons-java:0.2.19 org.jvnet.mimepull:mimepull:1.9.11 org.geotools.ogc:net.opengis.ows:24.2 io.netty:netty:3.9.9.Final io.airlift:node:202 com.neovisionaries:nv-websocket-client:2.12 com.squareup.okhttp:okhttp:2.7.5 com.squareup.okhttp3:okhttp:3.9.0 com.squareup.okhttp3:okhttp-urlconnection:3.9.0 com.squareup.okio:okio:2.10.0 org.eclipse.emf:org.eclipse.emf.common:2.15.0 org.eclipse.emf:org.eclipse.emf.ecore:2.15.0 org.eclipse.emf:org.eclipse.emf.ecore.xmi:2.15.0 org.geotools.ogc:org.w3.xlink:24.2 org.glassfish.hk2:osgi-resource-locator:1.0.1 org.pcollections:pcollections:2.1.2

SFR	Rationale
	org.sonatype.plexus:plexus-cipher:1.7 org.codehaus.plexus:plexus-classworlds:2.4 org.codehaus.plexus:plexus-component-annotations:1.5.5 org.codehaus.plexus:plexus-container-default:1.5.5 org.codehaus.plexus:plexus-interpolation:1.14 org.sonatype.plexus:plexus-sec-dispatcher:1.3 org.codehaus.plexus:plexus-utils:2.0.6 com.facebook.presto:presto-array:0.217-fastutil8 com.facebook.presto:presto-client:0.217 com.facebook.presto:presto-geospatial:0.217 com.facebook.presto:presto-geospatial-toolkit:0.217 com.facebook.presto:presto-main:0.217 com.facebook.presto:presto-matching:0.217 com.facebook.presto:presto-memory:0.217 com.facebook.presto:presto-memory-context:0.217 com.facebook.presto:presto-parser:0.217 com.facebook.presto:presto-plugin-toolkit:0.217 com.facebook.presto:presto-spi:0.217 com.teradata:re2j-td:1.4 org.reactivestreams:reactive-streams:1.0.3 org.reflections:reflections:0.9.11 io.airlift.resolver:resolver:1.4 io.reactivex.rxjava2:rxjava:2.2.21 io.airlift:security:0.178 org.apache.shiro:shiro-cache:1.7.1 org.apache.shiro:shiro-config-core:1.7.1 org.apache.shiro:shiro-config-ogdl:1.7.1 org.apache.shiro:shiro-core:1.7.1 org.apache.shiro:shiro-crypto-cipher:1.7.1 org.apache.shiro:shiro-crypto-core:1.7.1 org.apache.shiro:shiro-crypto-hash:1.7.1 org.apache.shiro:shiro-ehcache:1.7.1 org.apache.shiro:shiro-event:1.7.1 org.apache.shiro:shiro-guice:1.7.1 org.apache.shiro:shiro-lang:1.7.1 si.uom:si-quantity:2.0.1 si.uom:si-units:2.0.1 org.slf4j:slf4j-api:1.7.30 org.slf4j:slf4j-log4j12:1.7.30 io.airlift:slice:0.40 org.yaml:snakeyaml:1.26 io.airlift:stats:202 org.jvnet.staxex:stax-ex:1.8 io.swagger:swagger-annotations:1.6.2 io.swagger:swagger-core:1.6.2 io.swagger:swagger-jaxrs:1.6.2

SFR	Rationale
	io.swagger:swagger-models:1.6.2 systems.uom:systems-common:2.0.1 io.airlift:trace-token:0.178 org.glassfish.jaxb:txw2:2.3.1 javax.measure:unit-api:2.0 io.airlift:units:1.6 tech.uom.lib:uom-lib-common:2.0 javax.validation:validation-api:2.0.1.Final org.apache.maven.wagon:wagon-provider-api:2.2 org.apache.xbean:xbean-reflect:3.4 xml-apis:xml-apis:1.4.01
FPT_IDV_EXT.1	The TOE is versioned with version information published in the installation RPM. The TOE versioning methodology is ”Major Version”.”Minor Version”.”Patch Level”. Extensive patch notes are included with each version of the administrative guidance document.
FTP_DIT_EXT.1	The TOE encrypts all transmitted data via HTTPS over TLS, in accordance with FCS_HTTPS_EXT.1 and FCS_TLSC_EXT.1. Communication between the TOE and a ZeroReveal Compute Fabric Server is via REST over mutually authenticated TLS. The TOE communicates with an authentication server using Lightweight Directory Access Protocol (LDAP) secured with TLS. Users communicate with the TOE through REST interfaces via HTTPS/TLS.
ALC_TSU_EXT.1	Enveil uses commercial software to automatically check for active CVEs in any third-party dependencies, as part of its software development and release process. The window between public disclosure of a vulnerability and availability of a security update on the package manager will be 14 - 90 days.

Table 13 TOE Summary Specification SFR Description