National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Venafi Trust Protection Platform v23.1

Report Number: CCEVS-VR-VID11434-2024

Dated: 07/29/2024

Version: 1.0

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Lisa Mitchell

Linda Morrison

Randy Heimann

Lori Sarem

The MITRE Corporation

Common Criteria Testing Laboratory

Elliot Keen

Adarsh Pandey

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Venafi Trust Protection Platform Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in July 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended and meets the assurance requirements of the *Protection Profile for Application Software*, version 1.4, dated 07 October 2021 [SWAPP], and *Functional Package for Secure Shell*, version 1.0, dated 13 May 2021 [SSHFP].

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the *Common Methodology for IT Security Evaluation* (Version 3.1, Rev. 5) for conformance to the *Common Criteria for IT Security Evaluation* (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the Protection Profile (PP). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Venafi Trust Protection Platform v23.1
Protection Profile	*Protection Profile for Application Software*, version 1.4, dated 22 April 2022 [SWAPP], *Functional Package for Secure Shell*, version 1.0, dated 13 May 2021 [SSHFP].
Security Target	*Venafi Trust Protection Platform v23.1 Security Target*, version 1.6
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Extended
Sponsor & Developer	Venafi
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Lisa Mitchell Linda Morrison Randy Heimann Lori Sarem

3 Architectural Information

3.1 TOE Overview and Description

Venafi Trust Protection Platform is a windows application that secures and protects keys and certificates. This protection improves security posture with increased visibility, threat intelligence, policy enforcement, and faster incident response for certificate-related outages and compromises leveraging misused keys and certificates.

The platform supports all Venafi products and provides native integration with thousands of applications and common APIs for the extensive security ecosystem. Shared and extensible services enable enterprises to gain complete visibility into their key and certificate inventory, identify certificate reputation, and establish a baseline. The entire issuance and renewal process can be automated with policy enforcement and workflows, enabling new encryption dependent applications to be scaled quickly. Trust Protection Platform keeps organizations secure, helping them comply with standards and remediate key and certificate misuse.

The description above provides a general description of the functionality provided by the Venafi Trust Protection Platform.

3.2 Physical Boundaries

The TOE boundary is the application software which runs on the host platform. The TOE is a Windows Application. For this evaluation the TOE runs on Windows Server 2016 Standard configured in FIPS mode running on a server with an Intel Xeon processor with AES-NI and PCLMULQDQ and SSSE 3. The Universal C Runtime must be installed. In addition to this the following Microsoft Internet Information (IIS) web server roles must be installed:

- Common HTTP Features\Static Content
- Common HTTP Features\Default Document
- Health and Diagnostics\HTTP Logging
- Health and Diagnostics\Logging Tools
- Health and Diagnostics\Request Monitor
- Health and Diagnostics\Tracing
- Security\Request Filtering
- Performance\Static Content Compression

It should be noted that this operating system is outside the TOE boundary.

The following third-party libraries come bundled with the TOE and are inside the TOE boundary.

- IronPython
- Chaos.NaCl
- Microsoft Intune CSR Validation
- Sustainsys Saml2
- Excelsior JET

- F5 iControl Assembly for .NET
- Bootstrap
- Backbone
- Underscore
- Jquery
- date.js
- dateRangePicker.js, dateRangePicker.css
- moment.js
- easyDate.js
- maskedInput.js
- browser.js
- jquery.timepicker.js
- Select2.js
- moment-timezone.js
- core.js
- dropzone.js
- JSON.Net
- ASP.NET Web Stack
- Sencha Ext JS
- Tigra Calendar
- Pretty-Print JSON
- D3.js
- chart.js
- mustache.js

The TOE provides three consoles for management:

- A web-based console that can be launched by connecting to the TOE using a browser.
- Venafi Configuration Console (VCC): A powerful Microsoft Management Console (MMC) is a snap-in console that allows an administrator to manage Venafi services, enable product components, configure database settings.
- WinAdmin: A Windows-based console that runs locally on the Trust Protection Platform server.

The TOE also uses an external database to store credentials, certificates, keys and log data. Microsoft SQL Server 2022 Developer is used in the evaluated configuration and Microsoft SQL Server 2014, 2016 SP2, 2017, and 2019 are also supported. This database is outside the boundary of the TOE and is only used for the storage of data. All data that is sent to the database is encrypted by the TOE and is stored in the database as cipherstrings. Decryption of data happens on the TOE after the data is retrieved from the database. The TOE supports local as well as a remote database.

The TOE provides following connections:

- The TOE leverages Microsoft's IIS to provide web services for User or Admin authentication to access the web-based console
- The TOE connects to a remote database securely over TLS
- The TOE acts as a client and connects securely with managed hosts over SSH
- The TOE acts as a client and connects securely over TLS to perform discovery services
- The TOE communicates with a CA server over HTTP to validate the presented server's certificate by retrieving CRLs

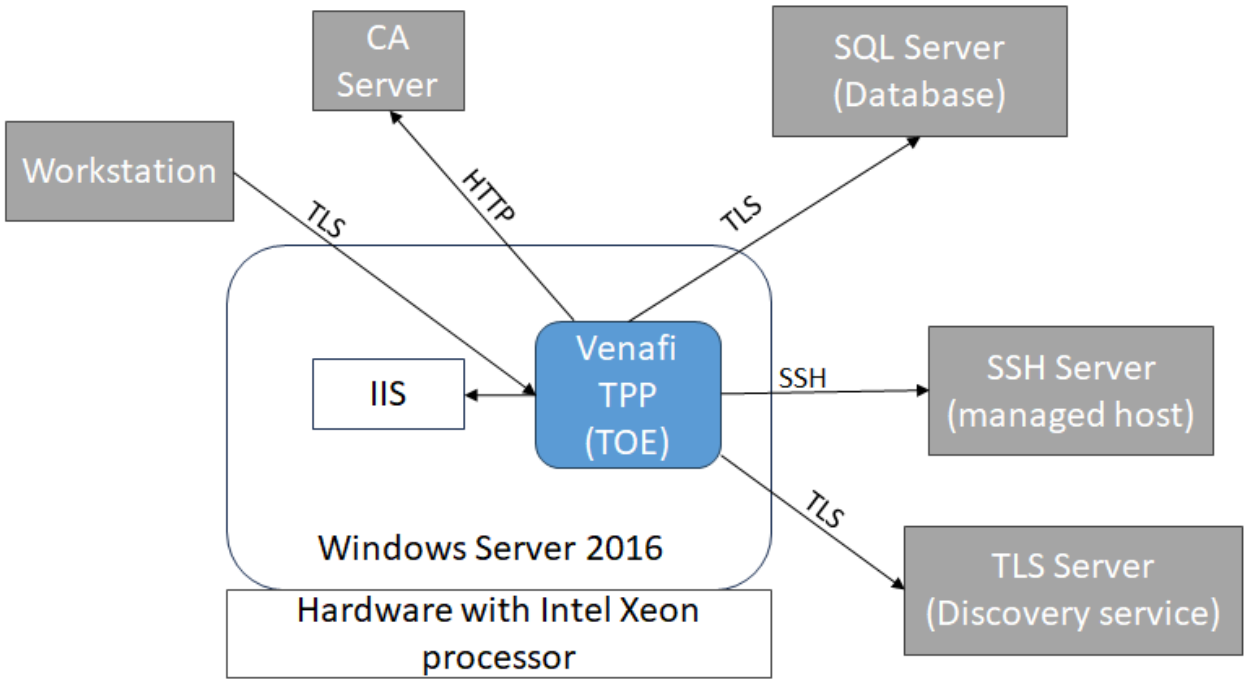

Figure 1 TOE network diagram

3.3 TOE Environment

The following components must be present in the operational environment to operate the TOE in the evaluated configuration:

Table 2 Operational Environment Components

Component	Required	Purpose/Description
Workstation	Optional	Workstation to access the TOE via web-based console over TLS.

SQL Server (Database)	Yes	The TOE uses an external database to store credentials, certificates, keys and log data. Microsoft SQL Server 2022 Developer is used in the evaluated configuration. The connection to a remote database is secured over TLS.
TLS Server (Discovery Service)	Optional	This is a IP-based target machine on which discovery services can be performed to discover the SSL certificates. The TOE communicates securely over TLS.
CA Server	Optional	This is a CRL server that provides a list of certificates that have been revoked. It is used by the TOE to check a server's presented certificate revocation status. The TOE communicates to the CA/CRL server over HTTP.
SSH Server (managed host)	Yes	This is a remote system managed host. TOE connects to the managed host over SSH

4 Security Policy

The TOE provides the security functionality required by [SWAPP] and [SSHFP].

4.1 Cryptographic Support

The TOE relies on underlying cryptographic functionality provided by the platform for all of its cryptographic operations, as allowed by the [SWAPP] and [SSHFP].

4.2 Security Management

The TOE does not come with any default credentials. Upon installation it will randomly generate a self-signed certificate, and AES 256 symmetric key and a GUID for the base configuration of the system. No data is stored by the application on the platform file system.

4.3 Privacy

The TOE does not store or transmit anything that could be considered Personally Identifiable Information (PII).

4.4 User Data Protection

The TOE relies on the platform to securely store the following:

- DSN key
- PKCS12 key
- PKCS8 (private key)
- Usernames
- Passwords
- Customer application credentials

The Windows Registry is used for storage of the TOE's symmetric key. An AES 256 key is used for the encryption and decryption of secrets. It is protected by the Windows Data Protection API (DPAPI).

No additional sensitive data is stored by the TOE.

4.5 Protection of the TSF

The TOE employs several mechanisms to ensure that it is secure on the host platform. The TOE never allocates memory with both write and execute permission. The TOE is designed to operate in an environment in which the following security techniques are in effect:

- Data execution prevention,
- Mandatory address space layout randomization (no memory map to an explicit address),
- Structured exception handler overwrite protection,
- Export address table access filtering, and
- Anti-Return Oriented Programming.

This allows the TOE to operate in an environment in which the Enhanced Mitigation Experience Toolkit is also running. During compilation, the TOE is built with several flags enabled that check for engineering flaws. The TOE is built with the /GS flag enabled. This reduces the possibilities of stack-based buffer overflows in the product.

4.6 Trusted Path/Channels

TLS and SSH are used to protect all data transmitted to and from the TOE.

5 Assumptions & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

The following assumptions are drawn directly from the SWAPP.

Table 3 Assumptions

ID	Assumption
A.PLATFORM	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 of the applied enterprise security policy.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in [SWAPP] and [SSHFP] as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within [SWAPP] and [SSHFP].
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Software Application models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities

to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- *Venafi Trust Protection Platform v23.1 Security Target*, Version 1.6 [ST]
- *Venafi Trust Protection Platform 23.1 Common Criteria Guidance*, Version 1.0 [AGD]

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in ETR for Venafi Trust Protection Platform, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the *Protection Profile for Application Software*, version 1.4, dated 22 April 2022 [SWAPP], and the *Functional Package for Secure Shell*, version 1.0, dated 13 May 2021 [SSHFP]. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE boundary is the application software which runs on the host platform. The TOE is a Windows Desktop/Classic Application. For this evaluation the TOE runs on Windows Server 2016 Standard configured in FIPS mode running on a server with an Intel Xeon processor with AES-NI and PCLMULQDQ and SSSE 3. The Universal C Runtime must be installed. In addition to this the following Microsoft Internet Information (IIS) web server roles must be installed:

- Common HTTP Features\Static Content
- Common HTTP Features\Default Document
- Health and Diagnostics\HTTP Logging
- Health and Diagnostics\Logging Tools
- Health and Diagnostics\Request Monitor
- Health and Diagnostics\Tracing
- Security\Request Filtering
- Performance\Static Content Compression

It should be noted that this operating system is outside the TOE boundary.

The following third-party libraries come bundled with the TOE and are inside the TOE boundary.

- IronPython
- Chaos.NaCl
- Microsoft Intune CSR Validation
- Sustainsys Saml2
- Excelsior JET
- F5 iControl Assembly for .NET
- Bootstrap
- Backbone
- Underscore
- Jquery
- date.js
- dateRangePicker.js, dateRangePicker.css
- moment.js
- easyDate.js
- maskedInput.js
- browser.js
- jquery.timepicker.js
- Select2.js
- moment-timezone.js
- core.js
- dropzone.js

- JSON.Net
- ASP.NET Web Stack
- Sencha Ext JS
- Tigra Calendar
- Pretty-Print JSON
- D3.js
- chart.js
- mustache.js

The TOE provides three consoles for management:

- A web-based console that can be launched by connecting to the TOE using a browser.
- Venafi Configuration Console (VCC): A powerful Microsoft Management Console (MMC) is a snap-in console that allows an administrator to manage Venafi services, enable product components, configure database settings.
- WinAdmin: A Windows-based console that runs locally on the Trust Protection Platform server.

The TOE also uses an external database to store credentials, certificates, keys and log data. Microsoft SQL Server 2022 Developer is used in the evaluated configuration and Microsoft SQL Server 2014, 2016 SP2, 2017, and 2019 are also supported. This database is outside the boundary of the TOE and is only used for the storage of data. All data that is sent to the database is encrypted by the TOE and is stored in the database as cipherstrings. Decryption of data happens on the TOE after the data is retrieved from the database. The TOE supports local as well as a remote database.

The TOE provides following connections:

- The TOE leverages Microsoft's IIS to provide web services for User or Admin authentication to access the web-based console
- The TOE connects to a remote database securely over TLS
- The TOE acts as a client and connects securely with managed hosts over SSH
- The TOE acts as a client and connects securely over TLS to perform discovery services
- The TOE communicates with a CA server over HTTP to validate the presented server's certificate (as part of TLS connection to the remote database or a discovery service)

8.2 Excluded Functionality

The following functionality is outside the scope of the evaluation:

- Providing visibility, threat intelligence, policy enforcement, and incident response for certificate-related outages and key compromises
- Integration with Venafi products and third-party applications – the evaluation is limited to secure communication channels
- Visibility into their key and certificate inventory, certificate reputation

- Issuance and renewal of certificates
- Policy enforcement
- Workflows
- Remediation of key and certificate misuse

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the ETR. The reader of this document can assume that all activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 Rev. 5 and CEM version 3.1 Rev. 5. The evaluation determined the Venafi Trust Protection Platform to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Venafi Trust Protection Platform that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in [SWAPP]/[SSHFP].

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in [SWAPP]/[SSHFP] related to the examination of the information contained in the TOE Summary Specification.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the

evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in [SWAPP]/[SSHFP] related to the examination of the information contained in the operational guidance documents.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

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

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in [SWAPP]/[SSHFP] and recorded the results in a Test Report, summarized in the ETR and AAR.

The validation team reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities on July 24, 2024, performed vulnerability testing and did not discover any issues with the TOE.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team suggests that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the SFRs specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

11 Annexes

Not applicable.

12 Security Target

Venafi Trust Protection Platform v23.1 Security Target, Version 1.6 [ST]

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

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

1. *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model*, Version 3.1 Revision 5.
2. *Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements*, Version 3.1 Revision 5.
3. *Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements*, Version 3.1 Revision 5.
4. *Common Evaluation Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 5.
5. *Protection Profile for Application Software*, version 1.4, dated 07 October 2021 [SWAPP].
6. *Functional Package for Secure Shell*, version 1.0, dated 13 May 2021 [SSHFP].
7. *Evaluation Technical Report for Venafi Trust Protection Platform v23.1*, Version 0.9 [ETR].
8. *Venafi Trust Protection Platform v23.1 Security Target*, Version 1.6 [ST].
9. *Venafi Trust Protection Platform v23.1 Common Criteria Guidance*, Version 1.0 [AGD].
10. *Assurance Activity Report for Venafi Trust Protection Platform v23.1*, Version 1.2 [AAR].
11. *Venafi Trust Protection Platform v23.1 Test Report*, Version 2.0, 07/04/2024.
12. *Vulnerability Assessment for Venafi Trust Protection Platform*, Version 1.9, July 24, 2024.