National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Venafi Trust Protection Platform v19.2

Report Number:	**CCEVS-VR-VID11024-2019**
Dated:	**February 21, 2020**
Version:	**1.0**

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

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Patrick Mallett, PhD Lead Validator
John Butterworth: ECR Team
Michelle Carlson: ECR Team
Lisa Mitchell: ECR Team
Clare Olin: ECR Team
MITRE Corporation

Jerome Myers, PhD Senior Validator
Aerospace Corporation

Common Criteria Testing Laboratory

Kathleen Moyer
Kenji Yoshino
Rutwij Kulkarni
Danielle Canoles

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 v19.2 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 February 2020. 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 Conformant and meets the assurance requirements defined in the Protection Profile for Application Software (SWAPP) version 1.3 and Extended Package for Secure Shell (SSHEP) version 1.0.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 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 SWAPP and SSH EP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report 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 Security Target (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 evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of 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 information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Venafi Trust Protection Platform v19.2.6
Protection Profile	Protection Profile for Application Software (SWAPP) version 1.3 Extended Package for Secure Shell (SSHEP) version 1.0
Security Target	Venafi Trust Protection Platform v19.2 Security Target v3.1, 2/19/2020
Evaluation Technical Report	Venafi Trust Protection Platform v19.2 ETR
CC Version	Version 3.1 Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Venafi
Developer	Venafi
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd Suite 395 Rockville, MD 20850
CCEVS Validators	Patrick Mallett, Jerome Myers, John Butterworth, Michelle Carlson, Lisa Mitchell, Clare Olin

3 Architectural Information

Venafi Trust Protection Platform secures and protects keys and certificates in the datacenter, on desktops, on mobile and IoT devices, and in the cloud. 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.

4 Security Policy

The logical boundary of the TOE includes those security functions implemented exclusively by the TOE.

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

Cryptographic Support

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

Secure Software Update

The TOE is distributed as a .MSI installer package.

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.

User Data Protection

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

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.

Trusted Path/Channels

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

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

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

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 of the applied enterprise security policy.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

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.

[1] ST Application Note: This Assumption has been updated according to TD0427.

5.3 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the SWAPPv1.3 and SSHEPv1.0.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation, specifically:
    - Securing and protecting keys and certificates
    - 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

6 Documentation

The following document was provided by the vendor with the TOE for evaluation:

- Venafi Trust Protection Platform v19.2 Common Criteria and FIPS Evaluated Configuration Guide v1.1, 2/5/2020.

Only the Configuration Guide listed above, and the specific sections of the other documents referenced by that guide should be trusted for the installation, administration, and use of this product in its evaluated configuration.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The evaluated configuration consists of application software configured in accordance with the documentation specified in Section 6. The TOE boundary is the application software which runs on the host platform. For this evaluation the TOE runs on Windows Server 2012 R2. 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.

A list of third-party libraries that come bundled with the TOE and are inside the TOE boundary is listed in section 1.3.2.7 of the Security Target. However, as is noted in the Clarification of Scope Section (5.3 above) the general effectiveness of the functionality provided by those libraries was not covered by the scope of this evaluation.

The TOE also uses an external database to store credentials, certificates, keys and log data. Microsoft SQL Server 2012 SP2 is used in the evaluated configuration and Microsoft SQL Server 2014 and 2016 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.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Venafi Trust Protection Platform v19.2, which is not publicly available. The Assurance Activities Report provides a public overview of testing and the prescribed assurance activities.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the SWAPP and SSH EP. An overview of the configurations used to test the TOE and the specific test tools used may be found in Section 5.1 of the Assurance Activity Report. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not further duplicated here.

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 Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Venafi Trust Protection Platform v19.2 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Venafi Trust Protection Platform v19.2 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 the SWAPP and SSH EP.

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

9.2 Evaluation of Development Documentation

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

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, 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 the SWAPP and SSH EP related to the examination of the information contained in the operational guidance documents.

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

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the SWAPP and SSH EP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the SWAPP and SSH EP, 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, performed vulnerability testing and did not discover any issues with the TOE. The following search terms were used to discover potential vulnerabilities:

- Venafi
- Trust Platform v19.2
- JSON.Net
- PDFSharp
- MigraDoc
- HTMLAgility Pack
- MS Anti-Cross Site Scripting Library
- IronPython
- jQuery v3.4.1
- Moment JS v2.24.0
- Backbone JS v1.4.0
- Twitter bootstrap Apache v2
- Underscore
- Boost
- Beast
- JSON11
- Base64

- Cxxopts
- Chaos.NaCI

The evaluation lab examined each result provided from NVD and Exploit Search to determine if the current TOE version or component within the environment was vulnerable. The vulnerability searches were conducted on February 20, 2020. The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the SWAPPv1.3 and SSHEPv1.0, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

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

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the SWAPPv1.3 and SSHEPv1.0, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Venafi Trust Protection Platform v19.2 Common Criteria and FIPS Evaluated Configuration Guide v1.1, 2/5/2020 document. This evaluation only applies to the version of the TOE listed in Section 2, Table 1. Any other versions, either earlier or later, should be assessed independently of this evaluation. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness

11 Annexes

Not applicable.

12 Security Target

Venafi Trust Protection Platform v19.2 Security Target v3.1, 2/19/2020.

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 1.3, dated 01 March 2019 [SWAPP].
6. Extended Package for Secure Shell, version 1.0, dated 19 February 2016 [SSHEP].