National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Extended Package for Secure Shell, Version 1.0, February 19, 2016

Report Number: **CCEVS-VR-PP-0039**
Dated: **29 September 2017**
Version: **1.0**

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Acumen Security, LLC
18504 Office Park Dr.
Montgomery Village, MD 20886

Table of Contents

Table of Tables

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Security Requirements for Secure Shell (Version 1.0) Extended Package (EPSSH10). It presents a summary of the EPSSH10 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the EPSSH10 was performed concurrent with the first product evaluation against the EP's requirements. In this case the Target of Evaluation (TOE) for this first product was the Venafi Trust Protection Platform version 17.1. The evaluation was performed by the Acumen Security Inc. Common Criteria Testing Laboratory (CCTL) in Montgomery Village, MD, United States of America, and was completed in September 2017. This evaluation addressed the base requirements of the EPSSH10 as well as a selection-based requirement in the EP.

Additional review of the EP to confirm that it meets the claimed APE assurance requirements was performed independently by the VR author as part of the completion of this VR.

The evaluation determined that the EPSSH10 is both Common Criteria Part 2 Extended and Part 3 Conformant. The EP 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 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). Because the ST contains material drawn directly from the EPSSH10, performance of the majority of the ASE work units serves to satisfy the APE work units as well.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team found that the evaluation showed that the EPSSH10 meets the requirements of the APE components. These findings were confirmed by the VR author. The conclusions of the testing laboratory in the assurance activity report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the EP.

In order to promote thoroughness and efficiency, the evaluation of the EPSSH10 was performed concurrent with the first product evaluation against the EP. In this case the TOE for this first product was the Venafi Trust Protection Platforms version 17.1. The evaluation was performed by Acumen Security Inc. Common Criteria Testing Laboratory (CCTL) in Montgomery Village, Maryland, United States of America, and was completed in September 2017.

The EPSSH10 contains a set of "base" requirements that all conformant STs must include in addition to "Selection-Based" requirements. Selection-Based requirements are those that must be claimed only in certain situations, depending on the selections made in the base requirements.

Because these discretionary requirements may not be included in a particular ST, the initial use of the EP will address (in terms of the EP evaluation) the base requirements as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the EPSSH10 that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made.

The following identifies the EP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this EP, as well as subsequent evaluations that address additional optional requirements in the EPSSH10.

Protection Profile	*Extended Package for Secure Shell, Version 1.0, 19 February 2016*
ST (Base)	*Security Target for Venafi Trust Protection Platforms Security Target, Version 1.3, September 2017*
Assurance Activity Report (Base)	*Venafi Trust Protection Platform SWAPP Assurance Activity Report, Version 1.2, September 15, 2017*
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTL	Acumen Security, LLC, Montgomery Village, MD
CCEVS Validators	Jean Petty, Mitre Corporation
	Chris Thorpe, Mitre Corporation

3 EPSSH10 Description

The EPSSH10 is an EP that addresses secure remote login and other secure network services over an untrusted network. This EP describes the extended security functionality of SSH in terms of Common Criteria. This EP can extend the Protection Profiles for *Application Software*, *General-Purpose Operating Systems*, or *Mobile Device Management*. In this evaluation, this EP has been appropriately combined with the Application Software PP to include selection-based requirements in accordance with the selections and/or assignments made.

4 Security Problem Description and Objectives

4.1 Assumptions

There are no assumptions defined for this EP. The TSF described by this EP exists in tandem with the functionality contained within each of the base PPs and does not add or remove assumptions regardless of which base PP is claimed.

4.2 Threats

There are no additional threats defined in this EP. The functionality described in this EP is intended solely to address threats that already exist in each of the base PPs.

4.3 Organizational Security Policies

No organizational security policies have been defined for this EP.

4.4 Security Objectives

There are no TOE objectives defined for this EP.

5 Requirements

As indicated above, requirements in the EPSSH10 are comprised of the "base" requirements and "selection-based" requirements which are based on selections from the base requirements. The following table contains the "base" requirements that were validated as part of the evaluation.

Table 1: Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_COP.1(1): Cryptographic Operation (Encryption/Decryption)	Venafi Trust Protection Platform Security Target
	FCS_SSH_EXT.1: SSH Protocol	Venafi Trust Protection Platform Security Target

The table below lists the "**Selection-Based**" requirements.

Table 2: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_SSHC_EXT.1: SSH Client Protocol	Venafi Trust Protection Platform Security Target
	FCS_SSHS_EXT.1: SSH Server Protocol	PP Evaluation

6 Assurance Requirements

There are no assurance requirements specific to this EP. A TOE that includes this EP is evaluated against the assurance requirements defined by the claimed base PP.

7 Results of the evaluation

Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

Table 3: Results of the evaluation

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	Venafi Trust Protection Platform Security Target
APE_ECD.1	Pass	Venafi Trust Protection Platform Security Target
APE_INT.1	Pass	Venafi Trust Protection Platform Security Target

APE_OBJ.1	Pass	Venafi Trust Protection Platform Security Target
APE_REQ.1	Pass	Venafi Trust Protection Platform Security Target

8 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 as interpreted by the supplemental guidance in the EPSSH10 Assurance Activities to determine whether or not the claims made are justified.
- **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.

9 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 4, dated: September 2012.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 4, dated: September 2012.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 4, dated: September 2012.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 4, dated: September 2012.

[5] Acumen Security, LLC, *Venafi Trust Protection Platform SWAPP Assurance Activity Report*, Version 1.2, 15 September 2017.

[6] Acumen Security, LLC, *Venafi Trust Protection Platform Security Target*, Version 1.3, September 2017.

[7] *Extended Package for Secure Shell*, Version 1.0, 19 February 2016