**TrustCB B.V.**

TRUST AND VERIFY

# Certification Report

# Cyberark Privileged Access Manager – Linux Components including PSMP v14.0.0.14

| | |
|---|---|
| Sponsor and developer: | ***CyberArk Software Ltd.***<br>**9 Hapsagot St. Park Ofer 2, P.O. Box 3143**<br>**Petach-Tikva 4951040**<br>**Israel** |
| Evaluation facility: | ***SGS Brightsight B.V.***<br>**Brassersplein 2**<br>**2612 CT Delft**<br>**The Netherlands** |
| Report number: | **NSCIB-CC-2400011-01-CR** |
| Report version: | **1** |
| Project number: | **NSCIB-2400011-01** |
| Author(s): | **Brian Smithson** |
| Date: | **03 July 2024** |
| Number of pages: | **12** |
| Number of appendices: | **0** |

*Reproduction of this report is authorised only if the report is reproduced in its entirety.*

# CONTENTS

# Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

# Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

## International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

## European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

# 1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Cyberark Privileged Access Manager – Linux Components including PSMP v14.0.0.14. The developer of the Cyberark Privileged Access Manager – Linux Components including PSMP v14.0.0.14 is CyberArk Software Ltd. located in Petach-Tikva, Israel and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a software application that runs on the Linux Operating System (OS), and it is a part of the CyberArk Privileged Access Manager (PAM) Solution suite. The TOE is composed of the PAM component PSMP, which provides the functionality to establish SSH connection to remote devices. In its evaluated configuration, the TOE is a part of CyberArk's PAM Solution. PSMP is installed on a single instance of Red Hat Enterprise Linux (RHEL) 8. RHEL contains the required OpenSSL and OpenSSH Server packages that are required to secure communications with clients. PSMP contains the required OpenSSH Client package that is installed on the RHEL machine for communicating with remote targets.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 03-07-2024 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Cyberark Privileged Access Manager – Linux Components including PSMP v14.0.0.14, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Cyberark Privileged Access Manager – Linux Components including PSMP v14.0.0.14 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the assurance requirements listed in section 2.9 for the evaluated security functionality, and conforms to the *[PP_APP]*, *[PKG_TLS]*, and *[PKG_SSH]*.

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

# 2 Certification Results

## *2.1 Identification of Target of Evaluation*

The Target of Evaluation (TOE) for this evaluation is the Cyberark Privileged Access Manager – Linux Components including PSMP v14.0.0.14 from CyberArk Software Ltd. located in Petach-Tikva, Israel.

The TOE is comprised of the following main components:

| Delivery item type | Identifier | Version |
|---|---|---|
| Software | Cyberark Privileged Access Manager – Linux Components including PSMP v14.0.0.14 | PSMP v14.0.0.14 |

To ensure secure usage a set of guidance documents is provided, together with the Cyberark Privileged Access Manager – Linux Components including PSMP v14.0.0.14. For details, see 2.5 of this document.

## *2.2 Security Policy*

The TOE provides the following security functions:

### 2.2.1 Cryptographic Support

The TOE uses a CAVP-validated cryptographic algorithm provided by its OpenSSL FIPS Object Module with the CyberArk library. The library is used to support the establishment of trusted channels to protect data in transit. In the evaluated configuration, the TOE's cryptographic library is used by the OpenSSH Client to remote targets and the TLS client connection to the Digital Vault Server.

### 2.2.2 User Data Protection

The TOE stores sensitive information in the form of encrypted passwords in non-volatile memory. The TOE limits its access to only network connectivity when accessing the platform's hardware resources. The network connection is used for communications from the TOE to the Digital Vault Server, the TOE to the target devices, and the user to the TOE. The TOE also accesses the Digital Vault Server's sensitive information repository (Safes) when it needs to authenticate users or request root credentials.

### 2.2.3 Identification and Authentication

To validate the Digital Vault Server's certificate during the TLS handshake, the TOE implements functionality to validate X.509 certificates. The TOE uses a CRL to check certificate revocation status and does not establish a connection to the Digital Vault Server when the CRL is unavailable.

### 2.2.4 Security Management

The TOE is configured with default file permissions already in place and does not provide default credentials for user authentication. The TOE relies on the platform for storing and setting configuration options within its config files. Administrators are able to view the status of the TOE in addition to being able to start, stop, and restart it.

### 2.2.5 Privacy

The TOE does not store or transmit any Personally Identifiable Identification (PII).

### 2.2.6 Protection of the TSF

The TOE protects against exploitation by implementing address space layout randomization (ASLR) except for vesical and not allocating memory with both writing and execution. The TOE is also compatible with SELinux and is compiled with stack-based buffer overflow protection. It also stores user-modifiable files to directories that do not contain executable files. The TOE uses standard platform APIs and includes only the third-party libraries that it needs to perform its functionality. The TOE version can be checked using commands provided by the platform. Checking for updates to the TOE is reliant on the platform's functionally. Any update downloaded for the TOE must be installed using the platform's package manager. An administrator will install a public key from CyberArk that is used by the package manager to verify the integrity of any updates to the TOE.

### 2.2.7 Trusted Path

The TOE provides a trusted channel between itself and target devices over SSH using OpenSSH Client. The SSH software used by the TOE follows the Extended Package for Secure Shell. A trusted TLS channel is used between itself and the Digital Vault Server.

## *2.3 Assumptions and Clarification of Scope*

### 2.3.1 Assumptions

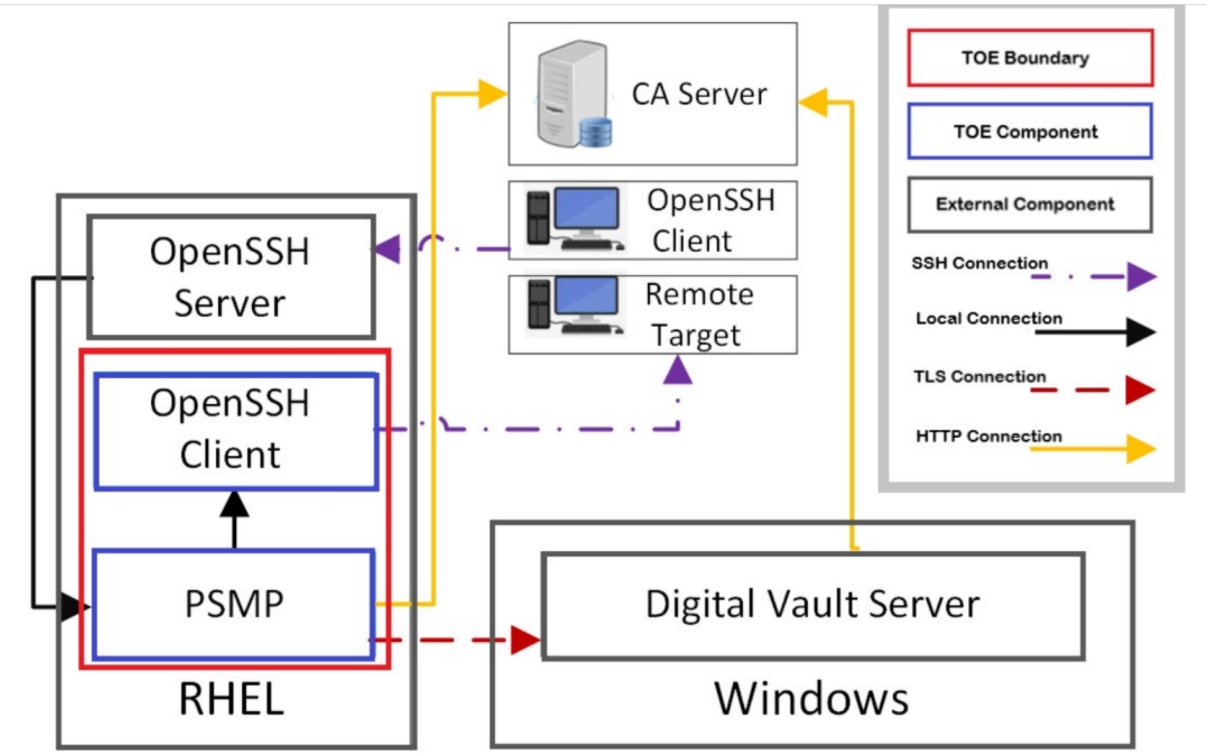
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 3.2 of the *[ST]*.

### 2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product

## *2.4 Architectural Information*

Below is a logical diagram of the TOE in its operational environment:



A user connects to PSMP by providing a target device, target user, Vault user, and Vault password, which are then relayed to the Digital Vault Server for verification. Once the user is verified, PSMP retrieves the target user's credentials to connect the user to the target device. While a user is connected to a target device and is performing activities in the privileged session, PSMP actively records all the activities and uploads them to the Digital Vault Server. PSMP is used to establish SSH connection to a remote target. PSMP separates the users from remote targets and stores the remote target's password in the Digital Vault. When a user connects to a remote target, PSMP retrieves the remote target's password from the Digital Vault using TLS through port 443, so PSMP enables connections to privileged devices without having to divulge the passwords to the user. PSMP logs user's activities that are performed in the privileged session and uploads the logs to the Digital Vault Server, where they are accessed by authorized users.

## *2.5 Documentation*

The following documentation is provided with the product by the developer to the customer:

| **Identifier** | **Version** |
|---|---|
| Privileged Access Manager – Linux Components Common Criteria Guide | V1.6, May 2024 |
| PAM Self-Hosted v14.0 | A8474D5E4B6532ED3402D38B46F7DB15F650CA75EBD0372BB891F3ECDC7089CE, 25-Jan-2024 |

## *2.6 IT Product Testing*

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

### 2.6.1 Testing approach and depth

Since the TOE conforms to *[PP_APP]* which requires exact conformance, all of the evaluator-defined tests are taken directly from *[PP_APP]*, *[PKG_TLS]*, and *[PKG_SSH]*. The evaluator performed all the tests on the TOE's version.

Some special crypto tests are performed on a special crypto library build. It is verified the special crypto build and the crypto library used in the TOE software is equivalent.

### 2.6.2 Independent penetration testing

The vulnerability assessment is performed following the guideline provided in [PP_APP], based on the following hypotheses:

- Type 1: Public – Vulnerability based
- Type 2: Tool Generated
- Type 3: Virus scanner

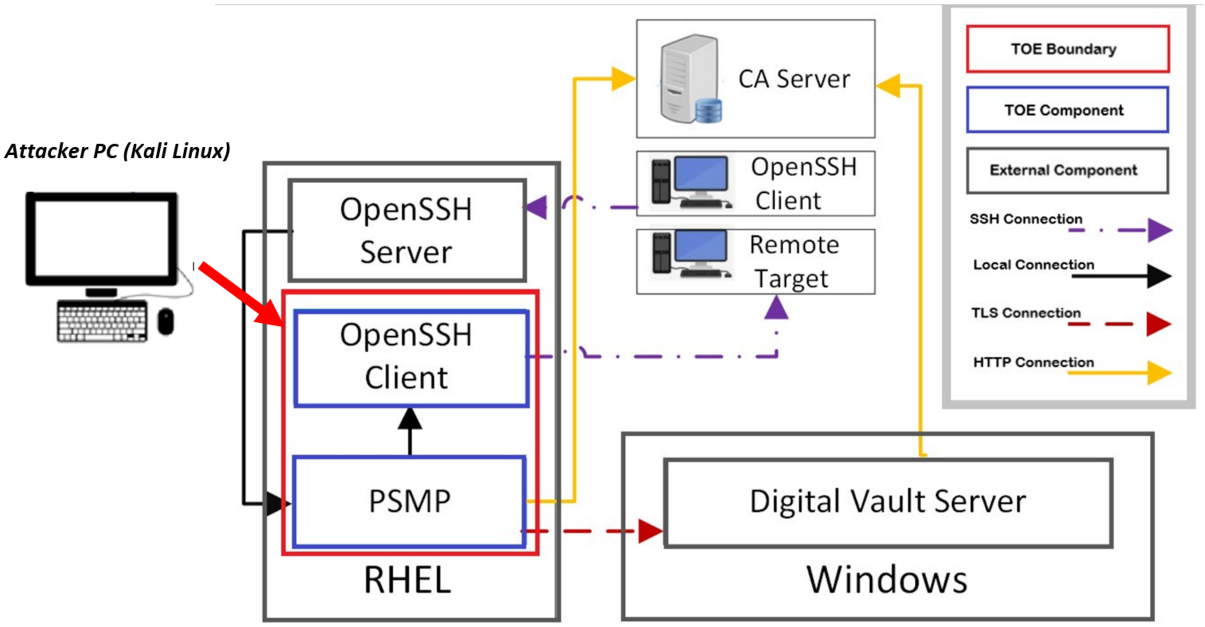
The evaluator performed all the tests (independent and penetration tests) in the period 17th March 2024 until 26th March 2024, with about 1 man-week (40 man-hour) in total for testing and reporting. During test campaign, 100% of the total time was spent on software (logical) attacks.

Penetration tests were created based on the vulnerabilities that are applicable to an attacker possessing a Basic attack potential and according to [PP_APP] work units of AVA_VAN.

No exploitable vulnerabilities were found.

### 2.6.3 Test configuration

Tests were executed as shown in the figure, below:



### 2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

## *2.7 Reused Evaluation Results*

There is no reuse of evaluation results in this certification.

## *2.8 Evaluated Configuration*

The TOE is defined uniquely by its name and version number Cyberark Privileged Access Manager – Linux Components including PSMP v14.0.0.14. Users must follow the guidance documents listed in section 2.5 of this document.

## *2.9 Evaluation Results*

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Cyberark Privileged Access Manager – Linux Components including PSMP v14.0.0.14, to be **CC Part 2 extended, CC Part 3 extended**, and to meet the requirements of **ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE.REQ.1, ASE.TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, and AVA_VAN.1**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims exact conformance to the Protection Profile *[PP_APP]*, and to the functional packages *[PKG_TLS]*, and *[PKG_SSH]*. All applicable NIAP Technical Decisions issued before 2024-06-01 have been addressed.

## 2.10 Comments/Recommendations

The user guidance as outlined in 2.5 of this document contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: **none**, which are out of scope as there are no security claims relating to these.

# 3 Security Target

The CyberArk Privileged Access Manager – Linux Components including Privileged Session Manager SSH (PSMP) v14.0 Security Target, (no doc ID), v1.9, 2024-06-13, *[ST]*, is included here by reference.

# 4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

| | |
|---|---|
| DVS | Digital Vault Server |
| IT | Information Technology |
| ITSEF | IT Security Evaluation Facility |
| JIL | Joint Interpretation Library |
| NSCIB | Netherlands Scheme for Certification in the area of IT Security |
| PAM | Privileged Access Manager |
| PP | Protection Profile |
| PSM | Privileged Session Manager |
| PSMP | Privileged Session Manager Proxy |
| SSH | Secure Shell |
| TOE | Target of Evaluation |

## 5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

| | |
|---|---|
| [CC] | Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017 |
| [CEM] | Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017 |
| [ETR] | CyberArk Privileged Access Manager Components v14.0 – Linux Component ETR, 24-RPT-356, v4.0, 2024-06-21 |
| [NSCIB] | Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022 |
| [PKG_SSH] | NIAP Functional Package for Secure Shell, v1.0, 2021-05-13 |
| [PKG_TLS] | NIAP Functional Package for Transport Layer Security, v1.1, 2019-03-01 |
| [PP_APP] | NIAP Protection Profile for Application Software, v1.4 (PP_APP), 2021-10-07 |
| [ST] | CyberArk Privileged Access Manager – Linux Components including Privileged Session Manager SSH (PSMP) v14.0 Security Target, (no doc ID), v1.9, 2024-06-13 |

(This is the end of this report.)