CyberArk Software Ltd.

Privileged Access Security – Linux Components

Including Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4

Guidance Documentation Supplement

Protection Profile for Application Software v1.2; April 22, 2016
Extended Package for Secure Shell (SSH) v1.0; 2016-02-19
Document Version: 0.9

Prepared for:

CyberArk Software Ltd.
9 Hapsagot St. Park Ofer 2
P.O.B. 3143
Petach-Tikva 4951040
Israel

Phone: +1 888 808 9005
www.cyberark.com

Prepared by:

Corsec Security, Inc.
13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2018-05-21	Lea Giovanniello Mark Kasulaitis	Initial draft.
0.2	2019-02-06	Mark Kasulaitis	Updated directions for version 10.4.
0.3	2019-03-12	Mark Kasulaitis	Updated directions for version 10.4.1.
0.4	2019-04-08	Mark Kasulaitis	Corrected the titles of the guides. Added the CA server to the list of OE servers. Added optional steps for using a client certificate in TLS. Updated the diagram. Updated the port settings. Corrected the OpenSSH parameters. Updated the patching/updating steps.
0.5	2019-04-13	Mark Kasulaitis	Steps have been updated to exclude some document references and include more instructions. Added a section for Network Restrictions.
0.6	2019-05-28	Mark Kasulaitis	Updated the information about checking for updates.
0.7	2019-08-12	Mark Kasulaitis	Updated the steps about checking for updates.
0.8	2019-08-28	Mark Kasulaitis	Updated the installation steps to include information about buffer overflow protection.
0.9	2020-12-16	Mark Kasulaitis	Updated the footer and removed the proprietary marking.

Table of Contents

List of Tables

List of Figures

1. Introduction

The Target of Evaluation (TOE) is the CyberArk Software Ltd. (CyberArk) Privileged Access Security – Linux Components, including Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4, and will hereafter be referred to as the TOE throughout this document. The TOE is a software-based solution that runs on Linux and is a component of CyberArk's Privileged Access Security (PAS) Solution. PAS enables organizations to secure, provision, control, and monitor all activities associated with privileged identities used in enterprise systems and applications. The PSMP enables organizations to secure, control, and monitor privileged access to network devices. OPM enables organizations to secure, control, and monitor privileged access to UNIX commands by allowing end users to perform super-user tasks with their own personal account without the need to know super-user credentials.

1.1 Purpose

This document provides guidance on the secure installation and secure use of the TOE for the Common Criteria (CC) Protection Profile for Application Software v1.2; April 22, 2016 (AS PP) and Extended Package for Secure Shell (SSH) v1.0; 2016-02-19 (SSH EP) evaluated configuration. This document provides clarifications and changes to the CyberArk documentation and should be used as the guiding document for the installation and administration of the TOE in the CC-evaluated configuration. The official CyberArk documentation should be referred to and followed only as directed within this document.

Table 1 below lists the guidance documents relevant to the installation and configuration of the TOE.

Table 1 – TOE Guidance Documents

Document Name	Description
CyberArk; Privileged Access Security Installation Guide	Includes steps for the basic initialization and setup of the TOE.
CyberArk; Privileged Access Security System Requirements	
CyberArk; Privileged Access Security End-user Guide	Contains detailed steps for how to properly configure and maintain the TOE.
CyberArk; Privileged Access Security Reference Guide	
CyberArk; Privileged Access Security Implementation Guide	

1.2 Target Audience

The audience for this document consists of the end-user, the CyberArk development staff, the Common Criteria Evaluation Laboratory staff, and the Government Certifier.

1.3 Evaluated TOE Configuration

Figure 1 depicts the evaluation configuration of the TOE. Acronyms used in the figure below that have not been previously identified are defined below.

- CA – Certificate Authority
- OpenSSH – Open Secure Shell
- TLS – Transport Layer Security
- RHEL – Red Hat Enterprise Linux
- R2 – Revision 2

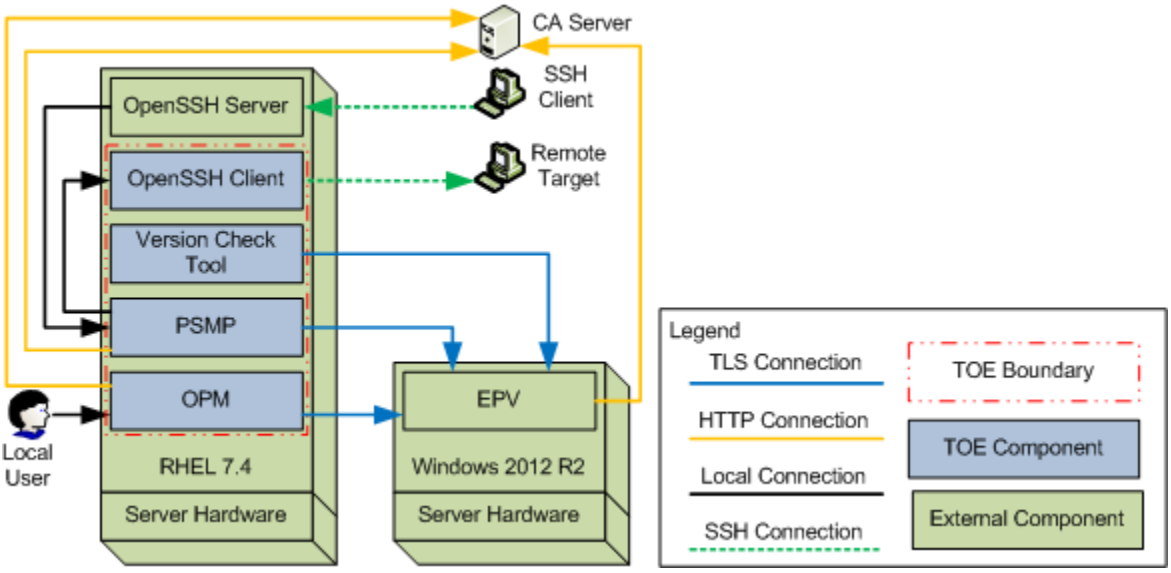

Figure 1 – Deployment Configuration of the TOE

1.4 Conventions

The following font conventions are used throughout this document:

- *Italics* font is used for *Document titles* included as reference.
- **Bold text** is used for navigation syntax and for general emphasis.
- **Bold text** is used for the bookmarked **section** and **subsections** from the *CyberArk Privileged Access Security Implementation Guide*.
- ***Bold italicized text paragraph header*** and the **">"** symbol are used for separating text within a **section** and **subsection(s).**

2. Installation Procedure

This section describes the installation procedure notes and changes.

2.1 Introduction

This section provides guidance for how to properly step through the installation instructions documented in the *Privileged Access Security Installation Guide*, along with additions and changes to the instructions contained therein, in order to allow the installer to properly install the evaluated configuration of the TOE.

Only users with root privileges can install the TOE. Before beginning the installation, the administrator must make certain that all the necessary platform components are in place. The *Privileged Access Security System Requirements* document contains the detailed requirements for all the components necessary to install the TOE. The following items are needed and must be acquired before continuing with this guidance:

- For the Vault server:
  - Microsoft Windows Server 2012 R2 operating system (OS)
  - Enterprise Password Vault (EPV) v10.4 software
  - .NET Framework 4.5.2
- For the RHEL Server:
  - RHEL 7.4 OS
  - PSMP v10.4
    - Including PSMP's OpenSSH Client
  - OPM v10.4
  - RHEL OpenSSH Server Cryptographic Module v5.0 containing OpenSSH Server 7.4p1-11.el7 (included in the RHEL installation)
  - RHEL OpenSSL Cryptographic Module v5.0 containing OpenSSL 1.0.2k-8.el7 (included in the RHEL installation)
  - Terminal
- For the workstation:
  - SSH client software such as plink, PuTTY, SecureCrt, etc.
- For the remote target:
  - SSH server software
- CA server:
  - Microsoft Windows Server 2012 R2 OS
  - Microsoft Active Directory (AD) Certificate Services (CS)

2.2 Secure Installation

Note: Throughout this section, the reader will be instructed to read certain passages from referenced documents. Unless otherwise stated, such instructions refer to the *Privileged Access Security Installation Guide*. For clarification, the *Privileged Access Security Installation Guide* will be explicitly referenced if used in the same paragraph with another referenced document. The Installation Guide does not have numeric references to sections and subsections and they are referenced in this document according to the conventions in section 1.4.

2.2.1 Phase 1 – Initial Preparation

Section 2.1 above specifies the required components for the evaluated configuration of the TOE and TOE environment. For more information on the evaluated configuration, please refer to section 1.4 of the *CyberArk Software Ltd. Privileged Access Security – Linux Components Security Target*. Before beginning, please review the **Considerations** section of the *Privileged Access Security Installation Guide*. The sections below contain information about configuring the TOE environment.

2.2.1.1 Initial Steps for Configuring the Vault Server

If not already done, please follow the *CyberArk Software Ltd.; Privileged Access Security – Digital Vault Server; Guidance Documentation Supplement* for installing and setting up the EPV server. This server will need to be setup before installing the TOE.

2.2.1.2 Initial Steps for Configuring the RHEL Server

When installing RHEL 7.4, please follow the RHEL 7.4 documentation located on the Red Hat website:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/installation_guide/index.

SELinux (Secure Linux) should already be installed and set to "Enforcing" by default, but if it is not, please enable SELinux as "Enforcing" by consulting the RHEL 7.4 SELinux User's and Administrator's Guide located on the Red Hat website:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/index

Terminal software should already be installed by default, but if a different application is desired, please follow the provider's documentation for installation or configuration.

2.2.1.3 Initial Steps for Configuring the CA Server

Please follow the Microsoft documentation for installing and setting up the CA server: https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/server-certificate-deployment.

The CA server will need to be setup to publish a CRL following one of the methods in the above Microsoft documentation. Please see section 3.1.2 below for a description of how the TOE components import the CRL from the CA server.

2.2.1.4 Initial Steps for Configuring the RHEL OpenSSH Server

Please follow the RHEL documentation for installing and setting up the RHEL OpenSSH Server package and RHEL OpenSSL package on the RHEL 7.4 server. The administrator should follow all guidance the FIPS security policies provided for each package. The security policy for the RHEL OpenSSH Server package is located on the National Institute of Standards and Technology (NIST) website here: https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3063.pdf. The security policy for the RHEL OpenSSL package is located on the NIST website here: https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3016.pdf. During installation of the PSMP component, the RHEL OpenSSH Server's configuration file is set to restrict access to only the allowed

algorithms. This ensures that only the allowed data integrity algorithms are used in SSH connections with the TOE and that the "none" value is not allowed for data integrity MAC[1] algorithms.

2.2.1.5 Initial Steps for Configuring the Workstation

When installing the SSH client software, please follow the provider's documentation for the system requirements and installation instructions.

2.2.1.6 Initial Steps for Configuring the Remote Target

When installing or configuring a remote target, please follow the provider's documentation for the installation or configuration instructions to enable the SSH connection. The settings of the target machine must be compatible with the SSH settings in Table 2 for the TOE to successfully connect to it.

2.2.1.7 Optional Steps for Generating a Client Certificate

A client certificate can be used between the TOE and the Vault Server. This is an optional step as it is not required for the TOE components to successfully communicate with the Vault Server. Create a client certificate by following the below steps:

1. Download the OpenSSL configuration file and edit the "[alt_names]" section to change the "IP.1" parameter to the real IP of the TOE's server.
2. Run the following OpenSSL commands:
   a. `openssl.exe genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out CertPrivate.key -aes-256-cbc -pass pass:[Passphrase]`
      i. Replace [Passphrase] with a secure password. This passphrase must be entered into the environment variable ENV_PASSPHRASE when you start the client as described in section 2.2.4.
   b. `openssl.exe req -new -key CertPrivate.key -config [Path of the edited openssl.cfg file] -out CertReq.csr`
3. Navigate to **https://<CA server IP>/certsrv** to obtain a cert for the TOE by following the below steps:
   a. Click on **Request a certificate**.
   b. Click on **Advanced certificate request**.
   c. Click on **Submit a certificate request…**
   d. Paste the contents of the CertReq.csr file into the **Saved Request** field.
   e. Choose a template that has the following:
      i. The Client Authentication key usage parameter.
      ii. The ability to receive the SAN parameter.
   f. Leave the **Attributes** field blank.
   g. Click on the **Submit** button.
   h. Download the certificate in Base64 encoding and save it as "CertClient.cer".
   i. The certificate (CertClient.cer) and its private key (CertPrivate.key) will be used as described in section 2.2.4.

[1] MAC – Message Authentication Code

2.2.2 Phase 2 – Download the TOE

From a browser on a workstation with access to the internet, use the CyberArk provided URL[2] and credentials to establish an HTTPS[3] session with CyberArk. Then download and save the TOE software that is listed in section 2.1. The downloaded files will have to be transferred to the TOE's server over the network or locally as the server will not have access to the internet to download the files itself.

2.2.3 Phase 3 – Verify the TOE

To verify the version of PSMP by file name, extract the files from the "PSM[4] CD[5] Image-Rls[6]-v10.4.1.zip" file and navigate to "\PSM CD Image\Privileged Session Manager SSH Proxy\". The .rpm[7] file is named "CARKpsmp-10.4.1-3.x86_64.rpm", indicating that it is version 10.4.1 of the PSMP.

To verify the version of OPM by file name, extract the files from the "OPM CD Image-Rls-v10.4.1.zip" file and navigate to "\OPM CD Image\RHELinux-Intel64\". The .rpm file is named "CARKaim-10.04.01.2.x86_64.rpm" indicating that it is version 10.4.1 of the OPM.

To verify CyberArk's digital signature on the PSMP .rpm file please follow the steps provided under the **Installing the Privileged Access Security Solution > Privileged Session Manager SSH Proxy > Before Installing PSMP > *Verify the installation package digital signature*** heading.

To verify CyberArk's digital signature on the OPM .rpm file please follow the steps provided under the **Installing the Privileged Access Security Solution > On-Demand Privileges Manager > Before Installation > *Verify the installation package digital signature*** heading.

2.2.4 Phase 4 – Install the TOE

Once the initial configuration of the TOE environment is completed in section 2.2.1 above and the TOE components are downloaded and verified, the TOE components may be installed on the RHEL server.

Please review the **Configuration Files > Privileged Session Manager SSH Proxy Parameter Files** and the **Configuration Files > On-Demand Privileges Manager Parameter Files** subsections for information about parameter settings.

2.2.4.1 PSMP Installation

To begin the PSMP installation, please follow the steps below:

1. On the PSMP machine, create a new directory for the installation files.
2. From the PSMP installation CD, copy the Privileged Session Manager SSH Proxy installation package to the new directory. Make sure to copy the folder and all its contents, including its subfolders.

[2] URL – Uniform Resource Locator
[3] HTTPS – Hypertext Transport Protocol Secure
[4] PSM – Privileged Session Manager
[5] CD – Compact Disk
[6] Rls – Release
[7] RPM – Red Hat Package Manager

3. Create the Credentials File for installation with the following steps:
    a. Run the following command to set execute permissions on the file: chmod 755 CreateCredFile
    b. Run the following command to launch the program: ./CreateCredFile user.cred
    c. Fill in the prompted information when asked. Refer to the **Create user credentials files** section of the *Installation Guide* for descriptions of each parameter.
4. Create the PSMP parameters file with the following steps:
    a. Move psmpparms.sample to the /var/tmp directory and rename it to psmpparms.
    b. Open the psmpparms configuration file and specify the following mandatory parameters:
        i. "InstallationFolder" should be set to the path to the PSMP folder that contains the vault.ini file.
        ii. "InstallCyberArkSSHD=Integrated"
        iii. "Hardening=Yes"
        iv. "AcceptCyberArkEULA=Yes"
5. Make the following changes to the vault.ini files:
    a. Set the "Address=" parameter to the address of the Vault server.
    b. Add "TLSPort=443".
    c. Set "Port" to an unused port (for example: "Port=1859")
    d. If the optional client certificate was created, add the following:
        i. ClientCertificate=[Path to the client certificate]
        ii. ClientCertificatePrivateKey=[Path to the client certificate's private key]
            1. Note that the private key must be in PKCS#8 format because this is the only accepted format while in FIPS mode.
6. If the optional client certificate was created, set the environment variable "ENV_PASSPHRASE" to the passphrase of the private key. The value is the passphrase used to unlock the TLS private key and must be entered before each of the PAS components startup.
7. From the PSMP folder, run the following command to start the installation: `sudo rpm –i <rpm-file-name>`. If any errors are seen during installation, refer to the **Troubleshoot the PSMP Installation** section of the *Installation Guide*.
    a. This step will install the software needed to allow buffer overflow protection in the environment. No extra steps are needed to setup the required software to enable buffer overflow protection and no specific configuration changes are needed to enable buffer overflow protection in the TOE as it is on by default.
8. Restart the sshd service.
9. Use the "rpm -q CARKpsmp" command from the terminal to display the installed PSMP filename and version**.**

2.2.4.2 OPM Installation

To begin the OPM installation, please follow the steps below.

1. Check if "policycoreutils-python" is installed by running the "rpm -q policycoreutils-python" command. If the output is blank or fails to find the package, run the "yum install policycoreutils-python" command to install as needed.
2. Check if "redhat-lsb" is installed by running the "rpm -q redhat-lsb" command. If the output is blank or fails to find the package, run the "yum install redhat-lsb" command to install as needed.
3. Create a new directory for the installation files.
4. From the CyberArk installation CD, copy the installation package to the new directory.
5. Create the Credentials File for installation with the following steps:

a. Run the following command to set execute permissions on the file: chmod 755 CreateCredFile
b. Run the following command to launch the program: ./CreateCredFile user.cred
c. Fill in the prompted information when asked. Refer to the **Create user credentials files** section of the *Installation Guide* for descriptions of each parameter.

6. Create the OPM parameters file with the following steps:
    a. Move aimparms.sample to the /var/tmp directory and rename it to aimparms.
    b. Open the aimparms configuration file and specify the following mandatory parameters:
        i. Change "LicensedProducts=<AIM,OPM,BOTH>" **to** "LicensedProducts=OPM".
        ii. Uncomment "HardenFSPermissions" and set it to Yes.
        iii. Uncomment "CreateVaultEnvironment" and set it to Yes.
        iv. Add the "AcceptCyberArkEULA" and set it to Yes.
        v. Set the "VaultFilePath" the path to the OPM folder that contains the vault.ini file.
7. Make the following changes to the vault.ini file:
    a. Set the "Address=" parameter to the address of the Vault server.
    b. Add "TLSPort=443" to the vault.ini file.
    c. Set "Port" to an unused port (for example: "Port=1859")
    d. If the optional client certificate was created, add the following:
        i. ClientCertificate=[Path to the client certificate]
        ii. ClientCertificatePrivateKey=[Path to the client certificate's private key]
            1. Note that the private key must be in PKCS#8 format because this is the only accepted format while in FIPS mode.
8. If the optional client certificate was created, set the environment variable "ENV_PASSPHRASE" to the passphrase of the private key. The value is the passphrase used to unlock the TLS private key and must be entered before each of the PAS components startup.
9. From the OPM folder, run the following command to start the installation: `sudo rpm -i <rpm-file-name>`. If any errors are seen during installation, refer to the **Troubleshoot the Installation** section of the *Installation Guide*.
10. Use the following commands to check that the OPM service is running: `/etc/rc.d/init.d/opmsrv status`
11. Use the "rpm -q CARKaim" command from the terminal to display the installed OPM filename and version**.**

2.2.5 Phase 5 – Post Installation

To complete the setup of the TOE and environment, please follow the steps in the sections below.

2.2.5.1 Configure OpenSSH Components

A hardened configuration is applied to the OpenSSH Client and Server components after the PSMP installation. Ensure that the values and parameters for the OpenSSH components match the specified ones in Table 2. These must be applied to the "/etc/ssh/sshd_config" and "/etc/ssh/ssh_config" files.

Table 2 – OpenSSH Hardening Parameters

Parameter	Value
Ciphers	aes128-ctr,aes256-ctr,aes128-cbc,aes256-cbc
HostbasedAcceptedKeyTypes (sshd_config) HostbasedKeyTypes (ssh_config)	ecdsa-sha2-nistp256,ecdsa-sha2-nistp384
HostKeyAlgorithms	ecdsa-sha2-nistp256,ecdsa-sha2-nistp384

Parameter	Value
KexAlgorithms	ecdh-sha2-nistp256,ecdh-sha2-nistp384
MACs	hmac-sha2-256,hmac-sha2-512
PubkeyAcceptedKeyTypes	ecdsa-sha2-nistp256,ecdsa-sha2-nistp384
RekeyLimit	1G 1h
PasswordAuthentication	no
GSSAPIAuthentication	no

2.2.5.2 Configure FIPS Mode for PSMP and OPM

FIPS mode is configured after installation of PSMP and OPM components. Please complete the steps below to configure FIPS mode for PSMP.

1. Create the following file: "/etc/opt/CARKpsmp/clients/clients.conf".
2. Edit the file and add "AdvancedFIPSCryptography=Yes".
3. Edit the "/etc/opt/CARKpsmp/conf/basic_psmpserver.conf" file and add "AdvancedFIPSCryptography=Yes".
4. Restart the PSMP service.

Please complete the steps below to configure FIPS mode for OPM.

1. Create the following file: "/etc/opt/CARKaim/clients/clients.conf"
2. Edit the file and add "AdvancedFIPSCryptography=Yes"
3. Edit the "/etc/opt/CARKaim/conf/basic_opm.conf" file and add "AdvancedFIPSCryptography=Yes".
4. Restart the OPM service.

2.2.5.3 Patches and Updates

The CyberArk Version Check tool is downloaded to the platform as part of the TOE and is used for checking updates to the TOE components. It relies on a file uploaded by the TOE administrator to the Vault server that contains all the current version information for the CyberArk PAS suite. The TOE administrator will also need to upload the update packages to the vault to allow for an internal update repository. Section 3.1.5 below will provide information about how and when to check for an update. The following steps are used to download and setup the tool:

1. Using a workstation with access to the external internet, connect to the CyberArk Support Vault and download the "CyberArk_Check_Version.zip" file located in the "CyberArk Documentation" Safe inside the "\Generic Technical information\Privileged Account Security\PAS" folder.
2. Also download the "PAS Latest Version.txt" file. This is a text file that contains only version information and it is not the update images for each component.
3. The most recent installation files must also be downloaded from the CyberArk Support Vault for all required PAS components. The update images will be separate archive (.zip) files.
4. Transfer the "CyberArk_Check_Version.zip" file to the TOE's host server and unzip the file.
5. Transfer the "PAS Latest Version.txt" and update files to the Vault Server and import them into a Safe.
6. Refer to section 3.1.5 below to check for updates.

3. Administrative Guidance

This section provides additional guidance not found in the guides listed in Table 1. Any clarifications, exclusions, or additions are detailed here to allow the TOE Administrator to properly configure and maintain the evaluated configuration of the TOE. The TOE Administrator should have successfully completed the installation procedures listed in section 2 before applying the guidance found in sections 3.1.

3.1 Clarifications

This section contains clarifications that need to be made to existing guidance documentation.

3.1.1 Password Complexity

The passwords defined for PSMP and OPM are used for CyberArk authentication and must meet the minimum password requirements for the EPV server. Please refer to the *Privileged Access Security – Digital Vault Server; Guidance Documentation Supplement* for the password complexity requirements.

3.1.2 Network Restrictions

Inbound and outbound communications are restricted to only TLSv1.2 communications between the Vault server and the TOE. During TOE installation, an administrator specifies port 443 for TLS communications. TOE hardening procedure closes all ports except ports 443 for TLS, 22 for SSH, and 80 for certificate revocation checking.

3.1.3 TLSv1.2 and X.509 Certificates

TLS is enabled by setting the value of the TLSPort parameter to “TLSPort=443”in PSMP’s and OPM’s vault.ini files in section 2.2 above. The TOE’s PSMP and OPM components are clients to the EPV server and each validates the EPV server’s X.509 certificate during TLS authentication. The components ensure that the X.509 certificate adheres to RFC 5280 (certificate validation and certificate path validation) and that the certificate path terminates with a trusted CA certificate. The components treat a certificate as a CA certificate when the certificate includes the basicConstraints extension and verifies that the CA flag is set to “TRUE” for all CA certificates. Each of the components validate the revocation status of the EPV’s TLS certificate according to RFC 5759 using a CRL when establishing the TLS connection. The path to the CRL is read from the certificate’s CRL Distribution Point (CDP) field, and the CRL is downloaded from the location. The PSMP and OPM components each check the EPV certificate against the downloaded CRL and automatically reject the certificate if it is found to be invalid. When a TLS v1.2 connection cannot be established because the validity check of a certificate fails, the connection is aborted. The PSMP and OPM components each validate the ExtendedKeyUsage field by ensuring that EPV certificate presented for TLS has the Server Authentication purpose in the extended key usage field.

3.1.4 PSMP Usage

Only the SCP[8] functionality of PSMP is used. Please refer to the *Privileged Access Security Implementation Guide's* **Working with the Privileged Access Solution Architecture > Account Access Workflows > Remote devices with X-forwarding >** ***Copy Files Securely Through the PSM SSH Proxy*** heading for more information about how to use SCP through PSMP.

3.1.5 Patches and Updates

An email notification from CyberArk will be sent to the TOE administrator when a new version is available. The TOE administration that receives the email notification is responsible for uploading the new version information and update files to the Vault server. The information in the email will contain the links to the appropriate download locations and the release notes related to the update. Since multiple components of the PAS solution check for updates against this central location, the administrator that uploads the files to the Vault server is responsible for maintaining accuracy of all component versions. The following process is used to upload the new files to the Vault Server and check for an update:

1. Using a workstation with access to the external internet, connect to the CyberArk Support Vault and download the "PAS Latest Version.txt" file located in the "CyberArk Documentation" Safe inside the "\Generic Technical information\Privileged Account Security\PAS" folder.
2. The most recent installation files must also be downloaded from the CyberArk Support Vault for all required PAS components.
3. Transfer the "PAS Latest Version.txt" and update files to the Vault Server and import them into the Safe where the original files were uploaded in section 2.2.5.3 above.
4. In the folder with the extracted files from section 2.2.5.3 above, run the **CA_CheckVersion.sh** bash script.
5. Fill in the information for each field that is displayed.
    a. The account used in the utility must have access to the Safe where the "PAS Latest Version.txt" file is stored.
6. Example the summary output to see the version information for the TOE.
    a. The utility will compare the version(s) of the installed CyberArk component(s) to the versions in the "PAS Latest Version.txt" file and display the results of the compression.
7. If the latest version is installed, the message will read "Product is up to date" and not further action is required.
8. If a new version is found, the message will read "2 products can be updated" and display the current and new version numbers.
    a. The new installation files will need to be transferred from the Vault Server's Safe to the TOE's host machine by the TOE administrator.
    b. The TOE administrator will use the steps in section 2.2.3 above to verify the signature on the update files.
    c. Installation of the update are preformed following the guidance provided in the **Upgrade** section of the *Privileged Access Security Installation Guide*.

The "PAS Latest Version.txt" file and update files will only need to be uploaded to the Vault Server whenever a new version is released. The TOE administrator will receive the email notification regarding every GA release of the TOE components that includes major, minor, and patch releases.

[8] SCP – Secure Copy Protocol

4. Acronyms

Table 3 defines the acronyms used throughout this document.

Table 3 – Acronyms

Acronym	Definition
AD	Active Directory
AIM	Application Identity Manager
AIX	Advanced Interactive eXecutive
AS PP	Protection Profile for Application Software v1.2; April 22, 2016
CA	Certificate Authority
CD	Compact Disk
CDP	Certificate Revocation List Distribution Point
CRL	Certificate Revocation List
EPV	Enterprise Password Vault
FIPS	Federal Information Processing Standard
HP-UX	Hewlett Packard – Unix
HTTPS	Hyper Text Transport Protocol Secure
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
NIST	Institute of Standards and Technology
OpenSSH	Open Secure Shell
OpenSSL	Open Secure Sockets Layer
OPM	On-Demand Privileges Manager
PAS	Privileged Access Security
PP	Protection Profile
PSM	Privileged Session Manager
PSMP	Privileged Session Manager SSH Proxy
RADIUS	Remote Authentication Dial-In User Services
RHEL	Red Hat Enterprise Linux
URLs	Release
RPM	Red Hat Package Manager
SCP	Secure Copy Protocol
SELinux	Secure Linux
SP	Service Pack

Acronym	Definition
SSH	Secure Shell
SSH EP	Extended Package for Secure Shell (SSH) v1.0; 2016-02-19
TLS	Transport Layer Security
TOE	Target of Evaluation
URL	Uniform Resource Locator

Prepared by:

Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com