CyberArk

Privileged Access Manager – Windows Components

Including Privileged Session Manager (PSM) v14.0, Central Policy Manager (CPM) v14.0, and Password Vault Web Access (PVWA) v14.0

Security Target

Version 1.8

Jun 2024

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Author	Description
0.1	09 Sept 2021	Marina Ibrishimova	First draft.
0.2	03 Nov 2021	Marina Ibrishimova	Updated ST to APP PP v1.4
0.3	19 Sep 2022	Marina Ibrishimova	Added latest TDs
0.4	09 Oct 2022	Marina Ibrishimova	Addressed vendor comments.
0.5	15 Jan 2023	Marina Ibrishimova	Addressed evaluator comments.
0.6	27 Feb 2023	Marina Ibrishimova	Addressed evaluator comments.
0.7	16 Apr 2023	Marina Ibrishimova	Addressed evaluator comments.
0.8	25 Apr 2023	Marina Ibrishimova	Addressed ALC observations.
0.9	11 Oct 2023	Marina Ibrishimova	Added latest TDs.
1.0	16 Oct 2023	Marina Ibrishimova	Addressed vendor comments.
1.1	15 Dec 2023	Marina Ibrishimova	Addressed ASE observations.
1.2	24 Jan 2024	Enav Coresh	Addressed ASE observations.
1.3	30 Jan 2024	Enav Coresh	Addressed ASE observations.
1.4	11 Feb 2024	Enav Coresh	Addressed ASE observations.
1.5	18 Apr 2024	Marina Ibrishimova	Addressed ASE comments.
1.6	9 May 2024	Marina Ibrishimova	Addressed ASE comments.
1.7	16 May 2024	Marina Ibrishimova	Addressed ASE comments.
1.8	13 Jun 2024	Marina Ibrishimova	Addressed ASE comments.

Table of Contents

List of Tables

1 ST Introduction

1 This Security Target (ST) defines the CyberArk Privileged Access Manager – Windows Components Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The TOE is a software-based solution that runs on Windows and is a component of CyberArk's Privileged Access Manager (PAM) Solution. PAM enables organizations to secure, provision, control, and monitor all activities associated with privileged identities used in enterprise systems and applications.

3 The TOE is composed of the PAM components Privileged Session Manager (PSM), Password Vault Web Access (PVWA), and Central Policy Manager (CPM).

4 PSM is the part of PAM that enables organizations to secure, control, and monitor privileged access to network devices over RDP connections. CPM automatically enforces enterprise policies for password management. PVWA is the web interface of PAM that provides a single console for requesting, accessing, and managing privileged passwords throughout the environment.

1.1 ST and TOE References

Table 1: Evaluation identifiers

ST Title	CyberArk Software Ltd. Privileged Access Manager – Windows Components including Privileged Session Manager (PSM) v14.0, Central Policy Manager (CPM) v14.0, and Password Vault Web Access (PVWA) v14.0 Security Target
ST version	Version 1.8
ST Author	Lightship Security
ST Publication Date	Jun 13, 2024
TOE Reference	CyberArk Privileged Access Manager – Windows Components including PSM v14.0.0.9, CPM v14.0.0.9 and PVWA v14.0.0.32

1.2 TOE Overview

1.2.1 Type

5 The TOE is a software application that runs on the Windows Operating System (OS), and it is a part of CyberArk's Privileged Access Manager (PAM) Solution suite.

6 The TOE is composed of the PAM components PSM, PVWA, and CPM.

1.2.2 Usage

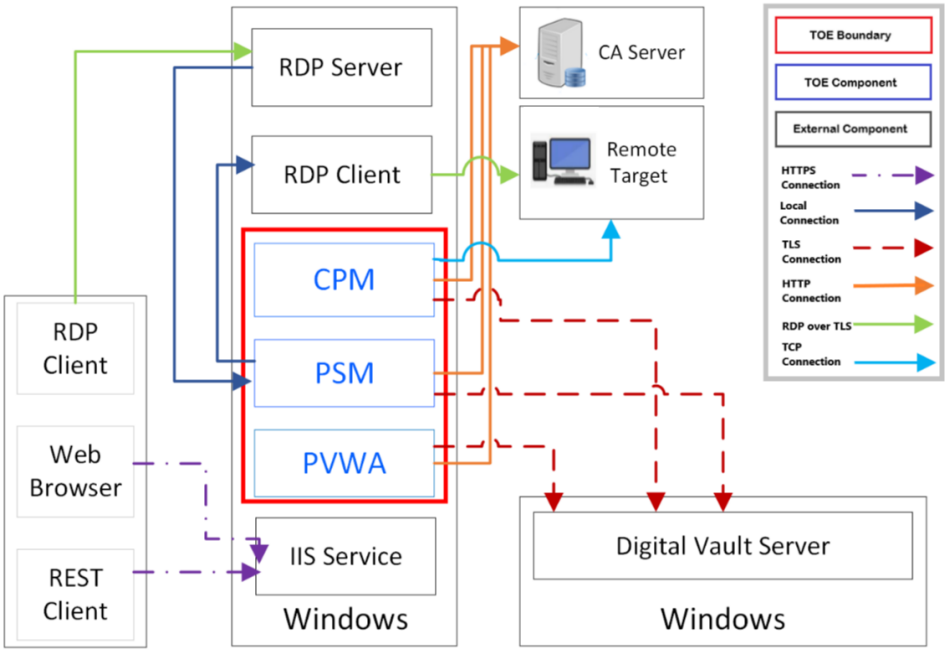
7 PVWA provides web-based administrator access to manage and configure PAM remotely over a web browser by providing access to policy and platform management features. PVWA identifies the administrator during authentication by checking the submitted credentials against what is stored in the Digital Vault Server or by having the Digital Vault Server check the credentials against the external

authentication server. The communication between PVWA and Digital Vault is conducted over TLS through port 443. PVWA is a standard web application, which runs on top of IIS.

8 PSM is used to establish RDP connection to a remote target. PSM 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, PSM retrieves the remote target's password from the Digital Vault using TLS through port 443, so PSM enables connections to privileged devices without having to divulge the passwords to the user. PSM records the activities that are performed in the privileged session and uploads the recording to the Digital Vault Server, where they are accessed and viewed by authorized users.

9 CPM enforces password policy. Administrators can configure security and compliance policies for all accounts' passwords. The policies, which specify minimum password requirements such as length, expiration, complexity, and others, are stored in the Digital Vault Server. CPM enforces policies by automatically changing passwords and storing the passwords within the Digital Vault Server. Each password changed by the CPM will be stored in Digital Vault and it will be updated in the remote target machine where this account exists. CPM uses a credential file to securely store its credentials to authenticate to Digital Vault, and once authenticated, CPM communicates with Digital Vault for retrieving and updating the passwords and password policies on the remote targets. The communication between CPM and Digital Vault is conducted over TLS through port 443.

Communication between the TOE components and the Digital Vault Server happens over TLS as shown in Figure 1.



10

Figure 1: TOE & Environment

1.2.2.1 Environment

11 It is assumed that there will be no untrusted users, administrators, or software on the TOE server component. Access to the server's OS must be limited to authorized personnel and secured with an authentication method. In addition, the TOE server

component is intended to be deployed in a physically secured cabinet, room, or data centre with the appropriate level of physical access control and physical protection (e.g., badge access, fire control, locks, alarms, etc.).

12 In the evaluated configuration, the TOE is a part of CyberArk's PAM Solution. PSM, CPM, and PVWA are installed on a single instance of Microsoft Windows Server 2019. IIS in the operating environment (OE) is used by PVWA for serving its web interface. PSM requires RDP services and RDP client in the OE for communicating with users and remote targets. An instance of Digital Vault Server is part of the OE and is installed on a standalone Windows 2019 server for access control usage by PSM, CPM, and PVWA.

13 To interact with the Digital Vault server, all TOE components require access to the same network in which the Digital Vault server is installed. Note that the platform that the TOE is installed on will not be allowed to have access to the internet and is intended for intranet use only. PSM will be used to connect to remote target in the OE using RDP. CPM will be used to rotate passwords to remote target in the OE. PVWA will be used to manage all accounts in the PAM solution.

14 CA server is used to validate the revocation list of TLS certificates, which are used by PSM, CPM and PVWA components, when communicating to Digital Vault over TLS.

1.2.3 Security Functions

15 The TOE provides the following security functions:

a) **Cryptographic Support.** The TOE uses the CAVP-validated cryptographic algorithm provided by its OpenSSL FIPS Object Module with CyberArk libraries. The libraries are used to support the establishment of trusted channels and paths to protect data in transit. In the evaluated configuration, the TOE's cryptographic libraries are used by the TLS client connection to the Digital Vault Server from PSM, CPM, and PVWA.

b) **User Data Protection.** The TOE encrypts all sensitive data stored in non-volatile memory. The TOE limits its access to 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/administrator to the TOE.

c) **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. The same functionality is used by CPM when it connects to the Digital Vault Server to manage passwords.

d) **Security Management.** The TOE is configured with default file permissions already in place and does not provide default credentials for authentication. The TOE relies on PVWA for storing and setting configuration options for PSM and CPM. Administrators can manage various parts of the TOE's functionality using the PVWA interfaces.

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

f) **Protection of the TSF.** The TOE leverages anti-exploitation capabilities provided by the OS. The TOE provides integrity for installation and software updates.

g) **Trusted Path.** The TOE relies on the IIS service in the OE to provide a trusted path for communications to the TOE using TLS. The TOE also relies on the RDP Client in the OE to provide a trusted channel for communications from the TOE to a remote target using TLS. The TOE provides its own trusted channel between each TOE component to the Digital Vault Server over TLS.

1.2.4 Non-TOE Components

16 The TOE operates with the following non-TOE components in the environment, which are intended to be deployed in a physically secure environment:

a) Digital Vault Server – Digital Vault, v14.0.0.40.

Digital Vault Server provides secure storage and access to privileged account files, and to the administrator and session activity files.

b) CA Server, Windows Server 2019, provides the functionality of downloading CRLs over HTTP

c) Windows 2019 Server, the server on which the TOE runs.

1.3 TOE Description

1.3.1 Physical Scope

17 The physical scope of the TOE is the Privileged Access Manger – Windows Components Windows application. The TOE includes Privileged Session Manager (PSM) v14.0.0.9, Central Policy Manager (CPM) v14.0.0.9, and Password Vault Web Access (PVWA) v14.0.0.32, and the TOE is delivered through CyberArk's online customer portal, which uses AWS Marketplace. The TOE delivery format is *.exe. The customer portal can be accessed after customers register to the portal https://cyberark.my.site.com/s/login.

18 Privileged Session Manager (PSM) executable version is CAPSM.exe, version 14.0.0.30. In order to install PSM, an installation package should be downloaded from CyberArk AWS marketplace, the version of the installation package is v14.0.0.9.

1.3.1.1 Guidance Parts

19 The TOE includes the following guidance documents, which are delivered to customers through a download link that becomes available to them after they purchase the TOE and sign in for the CyberArk Privileged Access Manager - Self-Hosted customer portal:

a) Privileged Access Manager – Windows Components Common Criteria Guide, v1.6 (PDF), May 2024

b) PAM Self-Hosted v14.0, 25-Jan-2024, No. A8474D5E4B6532ED3402D38B46F7DB15F650CA75EBD0372BB891F3ECDC7089CE, as follow:

Download the PAM Self hosted document described above >go to CyberArk Portal cyberark.my.site.com/mplace/s/#software > choose Privileged Access Manager Self-Hosted > go to Components > choose Documentation > download Production-PublicHelp-PAS - 14.0.zip and Extract > choose OnlineHelp.htm > choose Install and Harden components

a) Install: Installation > install PAM Self-Hosted

b) Upgrade: Installation > Upgrade

c) Admin: Administrator > Components

1.3.1.2 Configuration List

20 The evaluation package consists of the following:

a) Privileged Access Manager – Windows Components (TOE)

b) Privileged Access Manager – Windows Components Security Target, v1.8

c) Privileged Access Manager – Windows Components Common Criteria Guide, v1.6

d) Privileged Access Manager – Windows Components Entropy Description, v0.4

e) PAM Self-Hosted v14.0, 25-Jan-2024, No. A8474D5E4B6532ED3402D38B46F7DB15F650CA75EBD0372BB891F3ECDC7089CE

1.3.1.3 Out-of-Scope Functionalities

21 The out-of-scope functionalities are as follows:

a) PrivateArk client

b) PVWA:

i) Authentication other than LDAP or CyberArk are out of scope: SAML, Radius, OpenID out of scope.

ii) Ticketing system

iii) Oracle Database

iv) Check Point GAIA via SSH

v) DB2 on Unix via SSH

vi) Informix on Unix via SSH

vii) Microsoft SQL Server

viii) MySQL Server

ix) SAP HANA

x) Sybase ASE

xi) Cisco router via SSH

xii) Conjur host

xiii) Novell eDirectory server

xiv) SunOne directory via SSL

xv) Business Website

xvi) OS390 via SSH

c) Scanner

i) old autodetection

d) CPM

i) Supported engines: PMPassChange, NetInvoker

ii) TPC engine is out of scope.

e) PSM

i) PSM-SSH connection component
ii) PSM-WinScp connection component
iii) PSM-AS400 connection component
iv) PSM-OS390 connection component
v) PSM-SQLPlus connection component
vi) PSM-Toad connection component
vii) PSM-Telnet connection component
viii) PSM-PTA
ix) Distributed vault
x) Access control for Ad-Hoc connections
xi) PSM health check
xii) HTML5GW
xiii) PSM for Windows (aka RDP Proxy)
xiv) File transfer
xv) Live monitoring
xvi) External storage

1.3.2 Logical Scope

22 The logical scope of the TOE comprises the security functions defined in section 1 Security Functions.

1.4 Terminology

Table 2: Terminology

Term	Definition
CA	Certificate Authority
CC	Common Criteria
CPM	CyberArk Central Policy Manager
CRL	Certificate Revocation List
CDP	CRL distribution point
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
IIS	Internet information Services
LDAP	Lightweight Directory Access Protocol
OPM	CyberArk On-Demand Privileges Manager

Term	Definition
NIAP	National Information Assurance Partnership
PP	Protection Profile
PAM	CyberArk Privileged Access Manager
PSM	CyberArk Privileged Session Manager
PSMP	CyberArk Privileged Session Manager SSH (Secure Shell) Proxy
PVWA	CyberArk Password Vault Web Access
SRP	Secure Remote Password
TOE	Target of Evaluation
TSF	TOE Security Functionality

2 Conformance Claims

23 The following conformance claims are made:

1) CC version 3.1 Revision 5, April 2017
2) CC Part 2 extended, CCMB-2017-04-002, April 2017
3) CC Part 3 extended, CCMB-2017-04-003, April 2017
4) NIAP Protection Profile for Application Software, v1.4 (PP_APP), 2021-10-07
5) NIAP Functional Package for Transport Layer Security, v1.1, 2019-03-01, Conformant.
6) NIAP Technical Decisions per Table 3.

Table 3: NIAP Technical Decisions

TD Type	TD #	Name	Rationale if N/A
PP_APP	TD0628	Addition of Container Image to Package Format	
PP_APP	TD0650	Conformance claim sections updated to allow for MOD_VPNC_V2.3 and 2.4	
PP_APP	TD0664	Testing activity for FPT_TUD_EXT.2.2	
PP_APP	TD0717	Format changes for PP_APP_V1.4	
PP_APP	TD0719	ECD for PP APP V1.3 and 1.4	
PP_APP	TD0736	Number of elements for iterations of FCS_HTTPS_EXT.1	N/A. The TOE does not claim FCS_HTTPS_EXT.1/Server
PP_APP	TD0743	FTP_DIT_EXT.1.1 Selection exclusivity	
PP_APP	TD0747	Configuration Storage Option for Android	N/A. the TOE is not an Android app
PP_APP	TD0756	Update for platform-provided full disk encryption	
PP_APP	TD0780	FIA_X509_EXT.1 Test 4 Clarification	
PP_APP	TD0798	Static Memory Mapping Exceptions	
PP_APP	TD0815	Addition of Conditional TSS Activity for FPT_AEX_EXT.1.5	
PP_APP	TD0822	Correction to Windows Manifest File for FDP_DEC_EXT.1	
PP_APP	TD0823	Update to Microsoft Windows Exploit Protection link in FPT_AEX_EXT.1.3	
PKG_TLS_1.1	DT0779	Updated Session Resumption Support in TLS package V1.1	

TD Type	TD #	Name	Rationale if N/A
PKG_TLS_1.1	TD0770	TLSS.2 connection with no client cert	NA, this SFR is not claimed
PKG_TLS_1.1	TD0739	PKG_TLS_V1.1 has 2 different publication dates	
PKG_TLS_1.1	TD0726	Corrections to (D)TLSS SFRs in TLS 1.1 FP	
PKG_TLS_1.1	TD0513	CA Certificate loading	
PKG_TLS_1.1	TD0499	Testing with pinned certificates	
PKG_TLS_1.1	TD0469	Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1	
PKG_TLS_1.1	TD0442	Updated TLS Ciphersuites for TLS Package	

3 Security Problem Definition

24 The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any organizational security policies that the TOE is expected to enforce.

3.1 Threats

Table 4: Threats

Identifier	Description
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.

3.2 Assumptions

Table 5: Assumptions

Identifier	Description
A.PLATFORM	The TOE relies upon a trustworthy computing platform 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 within compliance of the applied enterprise security policy.

3.3 Organizational Security Policies

25 There are no organizational security policies for the application.

4 Security Objectives

4.1 Objectives for the TOE

Table 6: Security Objectives

Identifier	Description
O.INTEGRITY	Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom, if ever, shipped without errors. The ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options.
O.QUALITY	To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs.
O.MANAGEMENT	To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII.
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data.
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application.

4.2 Objectives for the Operational Environment

Table 7: Operational environment objectives

Identifier	Description
OE.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
OE.PROPER_USER	The user of the application software is not wilfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.
OE.PROPER_ADMIN	The administrator of the application software is not careless, wilfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

5 Security Requirements

5.1 Conventions

26 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text in square brackets.

b) **Refinement.** Indicated with bold text and strikethroughs in square brackets.

c) **Selection.** Indicated with underlined text in square brackets.

d) **Assignment within a selection.** Indicated with italicized and underlined text in square brackets.

e) **Iteration.** Indicated by adding a slash and a name, e.g., “FCS_COP.1/Hash”.

5.2 Extended Components Definition

27 All extended components (identified by EXT) are reproduced directly from the claimed Protection Profile and therefore no further definition is provided in this document.

5.3 Functional Requirements

Table 8: Summary of SFRs

Requirement	Title	Type
FCS_CKM.1/AK	Cryptographic Asymmetric Key Generation	Selection
FCS_CKM_EXT.1	Cryptographic Key Generation Services	Mandatory
FCS_CKM.2	Cryptographic Key Establishment	Selection
FCS_COP.1/SKC	Cryptographic Operation – Encryption/Decryption	Selection
FCS_COP.1/Hash	Cryptographic Operation – Hashing	Selection
FCS_COP.1/Sig	Cryptographic Operation – Signing	Selection
FCS_COP.1/KeyedHash	Cryptographic Operation – Keyed-Hash Message Authentication	Selection
FCS_RBG_EXT.1	Random Bit Generation Services	Mandatory
FCS_STO_EXT.1	Storage of Credentials	Mandatory
FCS_TLS_EXT.1	TLS Protocol	Mandatory
FCS_TLSC_EXT.1	TLS Client Protocol	Selection

Requirement	Title	Type
FCS_TLSC_EXT.5	TLS Client Support for Supported Groups Extension	Selection
FDP_DEC_EXT.1	Access to Platform Resources	Mandatory
FDP_NET_EXT.1	Network Communications	Mandatory
FDP_DAR_EXT.1	Encryption Of Sensitive Application Data	Mandatory
FIA_X509_EXT.1	X.509 Certificate Validation	Selection
FIA_X509_EXT.2	X.509 Certificate Authentication	Selection
FMT_MEC_EXT.1	Supported Configuration Mechanism	Mandatory
FMT_CFG_EXT.1	Secure by Default Configuration	Mandatory
FMT_SMF.1	Specification of Management Functions	Mandatory
FPR_ANO_EXT.1	User Consent for Transmission of Personally Identifiable Information	Mandatory
FPT_API_EXT.1	Use of Supported Services and APIs	Mandatory
FPT_AEX_EXT.1	Anti-Exploitation Capabilities	Mandatory
FPT_TUD_EXT.1	Integrity for Installation and Update	Mandatory
FPT_TUD_EXT.2	Integrity for Installation and Update	Selection
FPT_LIB_EXT.1	Use of Third-Party Libraries	Mandatory
FPT_IDV_EXT.1	Software Identification and Versions	Mandatory
FTP_DIT_EXT.1	Protection of Data in Transit	Mandatory

5.3.1 Cryptographic Support (FCS)

FCS_CKM.1/AK Cryptographic Asymmetric Key Generation

FCS_CKM.1.1/AK The application shall [implement functionality] **to** generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm [

- **[ECC schemes]** using **[“NIST curves” P-384 and [P-256]]** that meet the following: [**FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4**],

].

Application note: This SFR was changed by TD0717.

FCS_CKM_EXT.1 Cryptographic Key Generation Services

FCS_CKM_EXT.1.1 The application shall [implement asymmetric key generation].

Application Note: This SFR was altered by TD0717.

FCS_CKM.2 Cryptographic Key Establishment

FCS_CKM.2.1 The application shall [implement functionality] to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- [Elliptic curve-based key establishment schemes] that meets the following: [NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"],
- [FFC Schemes using "safe-prime" groups] that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 7919]

].

FCS_COP.1/SKC Cryptographic Operation – Encryption/Decryption

FCS_COP.1.1/SKC The application shall perform [*encryption/decryption*] in accordance with a specified cryptographic algorithm [

- AES-CBC (as defined in NIST SP 800-38A) mode,
- AES-GCM (as defined in NIST SP 800-38D) mode,

] and cryptographic key sizes [128-bit, 256-bit].

Application Note: This SFR was altered by TD0717.

FCS_COP.1/Hash Cryptographic Operation – Hashing

FCS_COP.1.1/Hash The application shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm [

- SHA-256,
- SHA-384,
- SHA-512

] and **message digest** sizes [

- 256,
- 384,
- 512

] **bits** that meet the following: [FIPS Pub 180-4].

Application Note: This SFR was altered by TD0717.

FCS_COP.1/Sig Cryptographic Operation – Signing

FCS_COP.1.1/Sig The **application** shall perform [*cryptographic signature services (generation and verification)*] in accordance with a specified cryptographic algorithm [

- **RSA schemes** using cryptographic key sizes of [2048-bit or greater] that meet the following: [FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5].

].

Application Note: This SFR was altered by TD0717.

FCS_COP.1/KeyedHash Cryptographic Operation – Keyed-Hash Message Authentication

FCS_COP.1.1/KeyedHash The **application** shall perform [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm [

- HMAC-SHA-256
- HMAC-SHA-384
- HMAC-SHA-512

] and [

- no other algorithms

] **with** key sizes [*256, 384, 512*] **and message digest sizes** [256, 384, 512] **and** [no other size] **bits** that meet the following: [*FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code' and FIPS Pub 180-4 'Secure Hash Standard'*].

Application note: This SFR was altered by TD0717.

FCS_RBG_EXT.1 Random Bit Generation Services

FCS_RBG_EXT.1.1 The application shall [invoke platform-provided DRBG functionality] for its cryptographic operations.

FCS_STO_EXT.1 Storage of Credentials

FCS_STO_EXT.1.1 The application shall [

- invoke the functionality provided by the platform to securely store [*Certificates in windows store*],
- implement functionality to securely store [*file keys*] according to [FCS_COP.1/SKC]

] to non-volatile memory.

FCS_TLS_EXT.1 TLS Protocol

FCS_TLS_EXT.1.1 The product shall implement [

- TLS as a client

].

FCS_TLSC_EXT.1 TLS Client Protocol

FCS_TLSC_EXT.1.1 The product shall implement TLS 1.2 (RFC 5246) and [no earlier TLS versions] as a client that supports the cipher suites [

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as define in RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288

] and also supports functionality for [

- none

].

Application Note: This SFR was altered by TD0442.

FCS_TLSC_EXT.1.2 The application shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.3 The product shall not establish a trusted channel if the server certificate is invalid [with no exceptions].

FCS_TLSC_EXT.5 TLS Client Support for Supported Groups Extension

FCS_TLSC_EXT.5.1 The product shall present the Supported Groups Extension in the Client Hello with the supported groups [

- secp256r1.
- secp384r1

].

5.3.2 User Data Protection (FDP)

FDP_DEC_EXT.1 Access to Platform Resources

FDP_DEC_EXT.1.1 The application shall restrict its access to [

- network connectivity

].

FDP_DEC_EXT.1.2 The application shall restrict its access to [

- *[IIS logs, PVWA logs, CPM logs, PSM logs and event logs]*

] .

FDP_NET_EXT.1 Network Communications

FDP_NET_EXT.1.1 The application shall restrict network communication to [

- user-initiated communication for [*HTTPS over TLS connections to PVWA*],
- [*application-initiated RDP over TLS connections to targets and TLS connections to the Digital Vault Server, HTTP connections to the CA server for certification revocation checks*]

].

FDP_DAR_EXT.1 Encryption Of Sensitive Application Data

FDP_DAR_EXT.1.1 The application shall [

- leverage platform-provided functionality to encrypt sensitive data,
- protect sensitive data in accordance with FCS_STO_EXT.1,

] in non-volatile memory.

5.3.3 Identification and Authentication (FIA)

FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1 The application shall [invoked platform-provided functionality, implement functionality] to validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The application shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.

- The application shall validate that any CA certificate includes caSigning purpose in the key usage field
- The application shall validate the revocation status of the certificate using [CRL as specified in RFC 5280 Section 6.3].
- The application shall validate the extendedKeyUsage field according to the following rules:
    - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing Purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
    - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the EKU field.
    - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field.
    - S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the EKU field.
    - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field.
    - Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.

FIA_X509_EXT.1.2 The application shall treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [TLS].

FIA_X509_EXT.2.2 When the application cannot establish a connection to determine the validity of a certificate, the application shall [not accept the certificate].

5.3.4 Security Management (FMT)

FMT_MEC_EXT.1 Supported Configuration Mechanism

FMT_MEC_EXT.1.1 The application shall [invoke the mechanisms recommended by the platform vendor for storing and setting configuration options]

FMT_CFG_EXT.1 Secure by Default Configuration

FMT_CFG_EXT.1.1 The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2 The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions [

- [*user management, configuration management, password management, start/stop service*]

].

5.3.5 Privacy (FPR)

FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1.1 The application shall [

- not transmit PII over a network,

].

5.3.6 Protection of the TSF (FPT)

FPT_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1 The application shall use only documented platform APIs.

FPT_AEX_EXT.1 Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1 The application shall not request to map memory at an explicit address except for [

- *0x00000000FB000000*

].

FPT_AEX_EXT.1.2 The application shall [not allocate any memory region with both write and execute permissions].

FPT_AEX_EXT.1.3 The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4 The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5 The application shall be built with stack-based buffer overflow protection enabled.

FPT_TUD_EXT.1 Integrity for Installation and Update

FPT_TUD_EXT.1.1 The application shall [leverage the platform] to check for updates and patches to the application software.

FPT_TUD_EXT.1.2 The application shall [provide the ability] to query the current version of the application software.

FPT_TUD_EXT.1.3 The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4 Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5 The application is distributed [as an additional software package to the platform OS].

FPT_TUD_EXT.2 Integrity for Installation and Update

FPT_TUD_EXT.2.1 The application shall be distributed using the format of the platform-supported package manager.

FPT_TUD_EXT.2.2 The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

FPT_TUD_EXT.2.3 The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.

FPT_LIB_EXT.1 Use of Third Party Libraries

FPT_LIB_EXT.1.1 The application shall be packaged with only [*the libraries outlined in Appendix B: List of Third-Party Libraries*].

FPT_IDV_EXT.1 Software Identification and Versions

FPT_IDV_EXT.1.1 The application shall be versioned with [[*version number*]].

5.3.7 Trusted Path/Channel (FTP)

FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1.1 The application shall [

- encrypt all transmitted [sensitive data] with [TLS as a client as defined in the Functional Package for TLS]

] between itself and another trusted IT product.

5.4 Assurance Requirements

28 The TOE security assurance requirements are summarized in Table 9.

Table 9: Assurance Requirements

Assurance Class	Components	Description
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.1	Security Objectives for the operational environment
	ASE_REQ.1	Stated Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM Coverage
	ALC_TSU_EXT.1	Timely Security Updates (as defined in PP_APP)
Tests	ATE_IND.1	Independent Testing – conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Analysis

6 TOE Summary Specification

6.1 Timely Security Updates

29 CyberArk endeavors to remediate critical and high severity publicly disclosed vulnerabilities in its TOEs, in accordance with their severity as implemented in the TOE, and subject to patches made available by their respective vendors (if applicable). The security updated can be provided as quickly as 4 weeks.

30 CyberArk will report a vulnerability to its customers when customers are required to take action to apply the remediation. Reporting of vulnerability-related issues may be via a security bulletin, release notes, knowledge base article, in-product notification or any other appropriate notification method. For the protection of CyberArk's customers, reporting of a vulnerability (including disclosure to any individual customer) will only be made once a remediation is made generally available by CyberArk, unless otherwise required by applicable law or regulation. In addition, the level of detail regarding a vulnerability in any reporting will be limited only to the minimum necessary.

31 If a security bulletin is issued, notification is sent via email to our technical subscribers (defined per customer upon request) and also published on the CyberArk website - Product Security | CyberArk, leading to a password-protected technical community - Login (site.com). First time users are asked to register prior to login.

6.2 SFR Fulfilment

32 Table 10 describes how the TOE fulfils the SFRs.

Table 10: SFR Fulfilment / TOE Summary Specification

SFR	Fulfilment
FCS_CKM.1/AK	Table 11 below lists all the key sizes used for the ECC asymmetric key generation scheme and its usage. Table 11 also lists the key establishment and key exchange schemes used by the TOE. The TOE uses ECDHE and DHE key establishment/exchange for TLS. The use of asymmetric encryption is needed for the TLS protocol used by the TOE. The key generation methods follow the requirements within FIPS PUB 186-4. The key establishment methods follow the requirements within NIST Special Publication 800-56A.
FCS_CKM_EXT.1	
FCS_CKM.2	
FCS_COP.1/SKC	AES 128-bit and 256-bit symmetric keys are used to encrypt/decrypt the TLS communications between the TOE and PAM components. AES is supported in CBC and GCM modes and used with 128-bit and 256-bit keys. AES256-CBC is used for the encryption/decryption of sensitive data stored in non-volatile memory.
FCS_COP.1/Hash	Table 12 lists all the key sizes used for SHA hashing and message digests within the TOE. Usages of SHA is limited to TLS and for SRP. The SHA256, SHA384, and SHA512 hash function are used in HMAC for TLS message integrity and authentication. The TOE's implementation of SHA follows the requirements within FIPS Pub 180-4

SFR	Fulfilment
FCS_COP.1/Sig	Table 11 lists all the key sizes used for signature generation and verification for TLS and the key sizes used to verify TOE file signatures. The TOE's implementation of signature generation and verification follow the requirements within FIPS PUB 186-4.
FCS_COP.1/KeyedHash	Table 12 lists all the key sizes used for SHA hashing and message digests within the TOE. Usage of SHA is limited to TLS and SRP. The SHA256, and SHA384, and SHA512 hash functions are used in HMAC for TLS message integrity and authentication. The TOE's implementation of SHA follows the requirements within FIPS Pub 180-4
FCS_RBG_EXT.1	The TOE implements the Approved SP 800-90 Approved AES256-CTR DRBG to generate random bits for key generation. When the TOE starts up, the DRBG is seeded with 256 bits of entropy from the Windows Entropy Pool by calling the **RAND_seed** function for the **BCryptGenRandom** function and for Windows Cryptography CNG (Cryptography Next Generation) API. The platform system time and tick count noise sources are added to the Windows OS Entropy Pool after initialization. On an ongoing basis the TOE seeds the DRBG with 256 bits of entropy by calling the **RAND_seed** function for the **BCryptGenRandom** function and for the Windows Cryptography CNG API. More information about the entropy process is described in the proprietary Entropy Rationale document.
FCS_STO_EXT.1	The TOE uses the Windows platform to securely store Certificates in the Windows store. The TOE encrypts file keys using 256-bit AES-GCM (as defined in NIST SP 800-38D).
FCS_TLS_EXT.1 FCS_TLSC_EXT.1	The TOE implements a TLS v1.2 client according to RFC 5246 using its CyberArk PAM TLS Library for Windows. This functionality is only used to communicate to the Digital Vault Server over TLS. Only the following cipher suite are suggested by the TOE for communications to the Digital Vault Server: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128-GCM-SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 From these, the Vault server does not support ECDSA certificates. From the remaining four suites, the vault server will always select the strongest one available, which is TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384. The TOE components communicate only with the Vault Server. Therefore, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 is the only ciphersuite used.

SFR	Fulfilment
	As part of establishing a TLS connection as a client, the TOE verifies that the presented identifier in the peer certificate is a valid reference identifier according to RFC 6125. The reference identifier is established by the TOE. The acceptable reference identifiers for the TOE are a Common Name or IP address for the Subject Name field. The Common Name field of the Digital Vault Server's certificate may contain its IP address because the Digital Vault Server is on a hardened machine that is not necessarily accessible via DNS43. The use of wildcards in the Subject Name is not supported. Certificate pinning is also not supported. The TOE will only establish a TLS connection if the peer certificate is valid.
FCS_TLSC_EXT.5	The TOE implements TLS v1.2 with support for EC44 algorithms. It supports the use of secp256r1 and secp384r1 EC Extensions to protect communications. The support of these curves is enabled by default for the TLS connection to the Digital Vault Server and configured during hardening of the server.
FDP_DEC_EXT.1 FDP_NET_EXT.1	The TOE limits its access to only network connectivity when accessing the platform's hardware resources. The TOE requires network access when workstations connect to the server over RDP with TLS and HTTPS or when the TOE server connects to the Digital Vault Server and remote targets over TLS. The user initiates a connection from their RDP Client over port 3389 when they want to connect to the PSM Client TSFI to be routed to a target machine. The user or administrator initiates a connection from their browser to IIS in the OE over port 443 using an HTTPS connection when they want to connect to the PVWA Client TSFI or PVWA RESTful API. This requires TOE to use the IIS service to use network resources. The TOE also uses port 80 for HTTP connections to the CA server for certification revocation checks from each component. When a user connects to the TOE for an RDP session, the TOE connects to the Digital Vault Server to verify their authentication information over TLS on port 443. If the authentication passes, PSM then connects to the target device using the RDP Client over a TLS connection on port 3389. PVWA connects to the Digital Vault Server over TLS on port 443 when it verifies authentication information through the PVWA Client TSFI or PVWA RESTful API. PVWA also connects to the Digital Vault Server over TLS on port 443 when it needs to update configuration settings for the PAM components. CPM connects to the Digital Vault Server over TLS on port 443 when it queries for updated password policies or changes an account's password. The TOE limits its access to sensitive IIS and event logs that are stored on and maintained by the platform.
FDP_DAR_EXT.1	Sensitive data within the TOE is limited to the passwords for service accounts. The TOE limits the storing of sensitive data in non-volatile memory to only passwords for the pvwaappuser, pvwagwuser,

SFR	Fulfilment
	passwordmanager, psmgw_, and psmapp_ service accounts. Each account's password is encrypted using AES256-CBC before it is saved. Other passwords that are used to authenticate with the Digital Vault Server are never stored in non-volatile memory by the TOE and transferred to and from the TOE over secure connections. PSM recordings may contain sensitive information if the user chooses to connect to a remote target which may contain sensitive information, therefore, we recommend the user to enable BitLocker.
FIA_X509_EXT.1	The TOE provides its own implementation of TLS to perform certificate validation. The TOE's PSM, CPM, and PVWA components are clients to the Digital Vault Server and each validates the Digital Vault Server's X.509v3 certificate during TLS authentication. The components ensure that the X.509v3 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 validates the revocation status of the Digital Vault Server's TLS certificate according to RFC 5759 using a CRL when establishing the TLS connection. The CRL is downloaded from the CA server in the operating environment. The path to the CRL is read from the certificate's CRL Distribution Point (CDP) field. The PSM, CPM, and PVWA components each check the Digital Vault Server 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 PSM, CPM, and PVWA components each validate that the Digital Vault Server's server certificate presented for TLS has the Server Authentication purpose in the extended key usage field. The TOE does not accept S/MIME, OCSP or EST certificates. The TOE supports a maximum trust depth of two nodes. Certificate validation is performed by the TOE, but if the certificate is not correct, Windows store will reject installing it.
FIA_X509_EXT.2	The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication. Each component of the TOE reads the location of their certificates from their vault.ini files using the ClientCertificate parameter. The TOE validates X.509v3 certificates from the Digital Vault Server for TLS authentication. This functionality is enabled by default. The path to the CRL is read from the certificate's CRL Distribution Point (CDP) field. The TOE's implementation of TLS automatically rejects a certificate if it is found to be invalid according to the requirements in FIA_X509_EXT.1. A certificate with an unknown revocation status due to the inability to establish a connection to the CDP is rejected. The connection from the TOE to the CDP is conducted over HTTP as per the RFC.

SFR	Fulfilment
FMT_MEC_EXT.1	The TOE does not write or set any configuration options using local configuration files. All configuration settings are stored in a Safe on the Digital Vault Server and can be configured using the PVWA interfaces. The TOE contains local configuration files that are created during installation, but the information is read-only and never written to by the TOE. Local configuration information related to the PSM component is stored in C:\Program Files (x86)\CyberArk\PSM\basic_psm.ini. Local configuration information related to the PVWA component is stored in the C:\inetpub\wwwroot\PasswordVault\web.config file. CPM does not provide a local configuration file.
FMT_CFG_EXT.1	No default credentials are provided by the TOE after the initial installation. Once the TOE is installed, it is connected to the Digital Vault Server for all authentication needs. The files created during installation are set with default permissions that do not allow the Users group to modify them. The files within the PSM's Oracle folder are automatically configured to allow the Users group read and execute permissions. All other PSM files do not allow the Users group any access. The files within the CPM and PVWA folders are automatically configured to allow the Users group read and execute permissions where needed.
FMT_SMF.1	The TOE provides the following management functions: user management, configuration management, password management, start/stop service. Any management operations must be performed by an authorized administrator using PVWA in the environment.
FPR_ANO_EXT.1	The TOE does not collect PII for administrators or users. Therefore, there is no case in which the TOE transmits this data over the network.
FPT_API_EXT.1	The TOE uses only the standard platform APIs. The list in Annex A: List of Platform APIs includes all the platform APIs used by the TOE. Note: The PVWA component of the TOE does not use any platform APIs.
FPT_AEX_EXT.1	The TOE does not request memory mappings at explicit addresses except for checking the hash value of the OpenSSL library. During the self-check in FIPS mode, the libeay32.dll are written to its respective memory address of 0x00000000FB000000 to allow the module to compute the correct hash of the libraries for comparison to known values. This mapped memory area has only read and execute permissions but no write permissions. When the TOE is being complied, it uses the **RandomizedBaseAddress** flag to enable ASLR. The TOE does not allocate any memory region with both write and execute permissions. No just-in-time compilations are performed by the TOE. The TOE is also compiled using the **/NXCOMPAT**"flag to enable Data Execution Protection (DEP) and the /**GS** flag to enable stack-based buffer overflow protection.

SFR	Fulfilment
	The TOE is installed on a hardened operating system based on Microsoft Bastion Host server recommendations. The TOE hardening is part of the installation and results in the disablement of many operating system services. The hardening process also strips the permissions from existing and built-in Windows accounts (except the account that runs the installation). For more information about the hardening process, refer to the *Harden the PSM server machine* section of the *CyberArk Installation Guide* and the *CyberArk Hardening the CyberArk CPM and PVWA Servers* document. The TOE does not write user-modifiable files to directories that contain executable files. User-modifiable files are written to the following folders: • C:\CyberArk\Password Vault Web Access\Services\Logs\ • C:\CyberArk\Password Vault Web Access\Env\Log\ • C:\Program Files (x86)\CyberArk\PasswordManager\Logs • C:\Program Files (x86)\CyberArk\PasswordManager\Scanner\Log • C:\Program Files (x86)\CyberArk\PSM\Logs
FPT_TUD_EXT.1/2 FPT_IDV_EXT.1	The TOE is delivered through CyberArk's online customer portal, which uses AWS Marketplace. The TOE installation and configuration files are all packaged into a zip file that is digitally signed by CyberArk. To verify the digital signature of a TOE package, users must do the following: 1. Download the TOE installation package from CyberArk. 2. Download and install the Java Development Kit (JDK) from Oracle. 3. Download and install the JCE Unlimited Strength Jurisdiction Policy Files. 4. Run the following command: **%JDK_Home%\jarsigner.exe -verify -verbose -certs .zip**. More information about the jarsigner's options can be found at https://docs.oracle.com/javase/7/docs/technotes/tools/windows/jarsigner.html#CCHFIDAB. Individual TOE files are signed using the Windows OS package manager MS21 Sign tool. To verify the integrity of the TOE installation file, do the following: 1. Extract the files from the archive file. 2. Navigate to the setup.exe file. 3. Right-click the file, then click **Properties** > **Digital Signatures**. 4. Select the **CyberArk Software Ltd.** signer. Click **Details**, and then verify the signature details. The authorized signing source is CyberArk. The TOE relies on the platform's package manager to make changes to the binary code. Installation of the updates is performed by an

SFR	Fulfilment
	administrator while using the executable file (.exe) extracted from the archive file (.zip). You can remove the TOE software from the platform using the platform's Programs and Features manager. Uninstallation of the TOE removes all traces of the application except for configuration settings, output files, and audit/log events. You can obtain the TOE version number by navigating to **C:\CyberArk\Server_rls**. Versioning naming convention: AA.B.C.DD (e.g: 14.0.0.32) - AA – Major Version Number – 14 - B – Minor Version Number – 0 - C – Patch Number – 0 - DD – Build Number – 32 Privileged Session Manager (PSM) executable version is CAPSM.exe, version 14.0.0.30. In order to install PSM, an installation package should be downloaded from CyberArk AWS marketplace, the version of the installation package is v14.0.0.9.
FPT_LIB_EXT.1	The TOE is packaged with third-party libraries required for its functionality as outlined in Appendix B: List of Third-Party Libraries
FTP_DIT_EXT.1	The TOE protects data in transit by providing trusted paths and channels using the cryptographic functions within the TOE's cryptographic libraries. The TOE provides a trusted TLS channel between itself and the Digital Vault Server. PSM, CPM, and PVWA are each able to negotiate a connection to the Digital Vault Server over TLS v1.2 when accessing Safes that are stored in Digital Vault Server. The OE provides a trusted path for communications using IIS when a user or administrator connects to the PVWA Client TSFI or PVWA RESTful API over HTTPS from their web browser or REST client respectively. This HTTPS connection is secured using TLS v1.2 and encrypted using AES-128-GCM, AES-256-GCM, AES-128-CBC, or AES-256- CBC depending on the cipher suite negotiated with the TLS client.

Table 11: Cryptographic Algorithms

Operation	Usage	Algorithm	Key Size
Encryption/Decryption	Secure Storage	AES-CBC	256

Operation	Usage	Algorithm	Key Size
	TLS	AES-GCM	128, 256
Key Generation	Safe	AES CTR-DRBG	256
Signature Generation Signature Verification	TLS	RSA	2048, 3072, 4096
Key Exchange /Establishment	TLS	ECDHE, DHE	256, 384 3072
Message Digest	TLS	SHA-256, SHA-384, SHA-512	256, 384, 512
Message Authentication	TLS	HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	256, 384, 512
Random Number Generation	TOE DRBG	CTR DRBG (AES)	N/A

Table 12: HMAC

Hash Function	Block Size	Key Length	Output Digest
SHA256	512	256	256
SHA384	1024	384	384
SHA512	1024	512	512

7 Rationale

7.1 Conformance Claim Rationale

33 The following rationale is presented with regard to the PP conformance claims:

a) **TOE type.** As identified in section 1.2.1, the TOE is an application, consistent with the PP.

b) **Security problem definition.** As shown in section 3, the threats, OSPs and assumptions are reproduced in this ST.

c) **Security objectives.** As shown in section 4, the security objectives are reproduced in this ST.

d) **Security requirements.** As shown in section 5, the security requirements are reproduced from the PP. No additional requirements have been specified.

7.2 Security Objectives Rationale

34 All security objectives are drawn directly from the claimed PP.

Table 13: Security Objectives Rationale

Threat, Assumption, or OSP	Security Objectives	Rationale
T.NETWORK_ATTACK	O.PROTECTED_COMMS, O.INTEGRITY, O.MANAGEMENT	The threat T.NETWORK_ATTACK is countered by O.PROTECTED_COMMS because this provides for integrity of transmitted data. The threat T.NETWORK_ATTACK is countered by O.INTEGRITY because this provides for integrity of software that is installed onto the system from the network. The threat T.NETWORK_ATTACK is countered by O.MANAGEMENT because this provides for the ability to configure the application to defend against network attack.
T.NETWORK_EAVESDROP	O.PROTECTED_COMMS, O.QUALITY, O.MANAGEMENT	The threat T.NETWORK_EAVESDROP is countered by O.PROTECTED_COMMS because this provides for confidentiality of transmitted data. The objective O.QUALITY ensures use of mechanisms that provide protection against network-based attack. The threat T.NETWORK_EAVESDROP is

Threat, Assumption, or OSP	Security Objectives	Rationale
		countered by O.MANAGEMENT because this provides for the ability to configure the application to protect the confidentiality of its transmitted data.
T.LOCAL_ATTACK	O.QUALITY	The objective O.QUALITY protects against the use of mechanisms that weaken the TOE with regard to attack by other software on the platform.
T.PHYSICAL_ACCESS	O.PROTECTED_STORAGE	The objective O.PROTECTED_STORAGE protects against unauthorized attempts to access physical storage used by the TOE.
A.PLATFORM	OE.PLATFORM	The operational environment objective OE.PLATFORM is realized through A.PLATFORM.
A.PROPER_USER	OE.PROPER_USER	The operational environment objective OE.PROPER_USER is realized through A.PROPER_USER.
A.PROPER_ADMIN	OE.PROPER_ADMIN	The operational environment objective OE.PROPER_ADMIN is realized through A.PROPER_ADMIN.

7.3 Security Requirements Rationale

35 All security requirements are drawn directly from the claimed PP.

Annex A: List of Platform APIs

PVWA: NA

CPM:

TCP Disconnect

QueryStandardInformationFile

WriteFile

TCP Receive

TCP Send

CreateFile

QueryDirectory

CloseFile

Thread Create

LockFile

ReadFile

UnlockFileSingle

QueryBasicInformationFile

QuerySecurityFile

TCP Connect

TCP Accept

RegQueryKey

RegOpenKey

RegCloseKey

RegCreateKey

RegSetInfoKey

RegQueryKeySecurity

RegQueryValue

RegEnumKey

TCP TCPCopy

CreateFileMapping

Thread Exit

Load Image

QueryNameInformationFile

FileSystemControl

QueryEAFile

Process Create

SetBasicInformationFile

PSM:

CloseFile

CreateFile

CreateFileMapping

FileSystemControl

Load Image

LockFile

Operation

Process Create

Process Exit

Process Start

QueryAllInformationFile

QueryAttributeTagFile

QueryBasicInformationFile

QueryDirectory

QueryEAFile

QueryInformationVolume

QueryNameInformationFile

QueryNetworkOpenInformationFile

QueryRemoteProtocolInformation

QuerySecurityFile

QuerySizeInformationVolume

QueryStandardInformationFile

ReadFile

RegCloseKey

RegCreateKey

RegEnumKey

RegEnumValue

RegOpenKey

RegQueryKey

RegQueryKeySecurity

RegQueryMultipleValueKey

RegQueryValue

RegSetInfoKey

RegSetValue

SetAllocationInformationFile

SetBasicInformationFile

SetDispositionInformationFile

SetEndOfFileInformationFile

SetRenameInformationFile

TCP Accept

TCP Connect

TCP Disconnect

TCP Receive

TCP Retransmit

TCP Send

TCP TCPCopy

Thread Create

Thread Exit

UnlockFileSingle

WriteFile

Appendix B: List of Third-Party Libraries

PVWA

utofac.dll

Autofac.Extras.DynamicProxy.dll

AutoMapper.dll

AWSSDK.CognitoIdentityProvider.dll

AWSSDK.Core.dll

AWSSDK.SecretsManager.dll

BouncyCastle.Crypto.dll

Castle.Core.dll

Common.Logging.Core.dll

Common.Logging.dll

ComponentSpace.SAML2.dll

DocumentFormat.OpenXml.dll

EasyNetQ.dll

IdentityModel.dll

InventoryReports.dll

Ionic.Zip.dll

log4net.dll

Marvin.JsonPatch.dll

Microsoft.AspNet.SignalR.Core.dll

Microsoft.AspNet.SignalR.SystemWeb.dll

Microsoft.Diagnostics.Tracing.EventSource.dll

Microsoft.IdentityModel.Abstractions.dll

Microsoft.IdentityModel.JsonWebTokens.dll

Microsoft.IdentityModel.Logging.dll

Microsoft.IdentityModel.Tokens.dll

Microsoft.Owin.dll

Microsoft.Owin.Host.SystemWeb.dll

Microsoft.Owin.Security.dll

Microsoft.Web.UI.WebControls.DLL

Newtonsoft.Json.dll

Owin.dll

PIMSuiteData.dll

PowerCollections.dll

Quartz.dll

RabbitMQ.Client.dll
Swashbuckle.Core.dll
Swashbuckle.Examples.dll
System.Buffers.dll
System.ComponentModel.Annotations.dll
System.Diagnostics.DiagnosticSource.dll
System.IdentityModel.Tokens.Jwt.dll
System.Memory.dll
System.Net.Http.Formatting.dll
System.Numerics.Vectors.dll
System.Runtime.CompilerServices.Unsafe.dll
System.Text.Encodings.Web.dll
System.ValueTuple.dll
System.Web.Extensions.dll
System.Web.Http.dll
System.Web.Http.WebHost.dll
VimService.dll
VimService.XmlSerializers.dll
WebChart.dll

CMP

AWSSDK.Core.dll
AWSSDK.IdentityManagement.dll
Castle.Core.dll
Castle.Windsor.dll
Eagle.dll
Expect.NET.dll

PSM

ComponentSpace.Saml2.dll
ComponentSpaceWrapper.dll
ComponentSpaceWrapperDotNet.dll
msvcp140.dll
Vault\log4cpp.dll
Components\Castle.Core.dll
Components\Castle.Windsor.dll
Components\Eagle.dll

Components\MinHook.x64.dll

Components\MinHook.x86.dll

Components\Otp.NET.dll

Components\SeleniumExtras.WaitHelpers.dll

Components\WebDriver.dll

Components\WebDriver.Support.dll