

CyberArk Integration

CyberArk - Status Report

Doküman No	PRO-KL001-G-04
Versiyon	0.4
Yayın Tarihi	01.12.2024

Revision History

Date	Description	Prepared by	Approved by	Version
1 November 2024	First draft	Murat YILDIZ	-	0.1

Table of Contents

Revision History 3

Introduction 4

1. What is CyberArk?..... 6

 1.1. Products That Can Be Used with HSM in CyberArk 6

2. What is CyberArk EPV (Enterprise Password Vault)? 7

3. CyberArk EPV HSM Integration..... 7

REFERENCES..... 12

1. What is CyberArk?

CyberArk is a cybersecurity company primarily focused on providing privileged access security solutions. The company's mission is to help organizations securely manage access to critical systems, data, and privileged accounts.

CyberArk's flagship product is the CyberArk Privileged Access Security (PAS) Suite. This solution offers capabilities to secure, monitor, and manage privileged access accounts, identities, and passwords. Privileged access accounts are those with special permissions within corporate networks and systems, granting access to sensitive data or critical systems. By protecting these accounts, CyberArk aims to prevent unauthorized access, mitigate data breaches, and reduce security risks.

While the CyberArk PAS Suite focuses on privileged access management, its other products cover areas such as privileged session management, password management, session recording, identity and access management, and more. These products enhance defenses against cyberattacks and ensure compliance by securing privileged access.

Overall, CyberArk's solutions are designed to help organizations achieve privileged access security, prevent data breaches, and reduce security risks. The company is a leading cybersecurity provider widely used by major organizations worldwide.

1.1. Products That Can Be Used with HSM in CyberArk

CyberArk provides HSM (Hardware Security Module) integration across various products. Below are some CyberArk products that support HSM integration:

- 1. CyberArk Enterprise Password Vault (EPV):**
EPV is a solution designed for the centralized storage, management, and control of access to sensitive credentials. With HSM integration, EPV can support HSM devices for key management and data security.
- 2. CyberArk Privileged Session Manager (PSM):**
PSM is a solution used to secure, monitor, and manage critical privileged sessions. With HSM integration, PSM can securely store privileged session recordings and utilize HSM devices for key management.
- 3. CyberArk Secrets Manager:**
Secrets Manager is a solution designed to control and monitor privileged access for applications, servers, and databases. With HSM integration, Secrets Manager can use HSM devices to securely store and manage privileged access keys and credentials.

This list provides examples of CyberArk products that support HSM integration. CyberArk's product portfolio is continually updated with new features and capabilities. Therefore, it is important to refer to the latest CyberArk documentation and product guides for specific products or solutions where you plan to implement HSM integration.

2. What is CyberArk EPV (Enterprise Password Vault)?

CyberArk Enterprise Password Vault (EPV) is software developed by CyberArk Corporation, designed to centrally store and manage an organization's sensitive credentials (particularly passwords). EPV enhances security and access controls, enabling efficient management of identities and credentials.



The primary purpose of EPV is to ensure the protection of critical account credentials. This software can be used to store, encrypt, and manage passwords, certificates, API keys, and other sensitive information. By restricting access to these credentials to a limited number of authorized individuals, organizations can enhance the security of their information.

EPV allows users to create strong and unique passwords and facilitates regular password changes. Additionally, by storing credentials and monitoring access, it enforces security policies to control who can access specific information.

CyberArk EPV is particularly suitable for organizations with large and complex IT infrastructures. It can be used to manage user accounts across multiple systems and applications, reducing security risks. The centralized password management and access control provided by EPV help protect against data breaches and can also be leveraged to meet regulatory compliance requirements.

3. CyberArk EPV HSM Integration

The following steps have been carried out sequentially to implement the HSM integration for CyberArk EPV:

- The CyberArk EPV Server is shut down to perform the necessary configuration within CyberArk EPV.

The screenshot shows the 'Server Central Administration' window. The 'Administration' tab is selected. The main area displays a list of system messages in a table with columns for Date, Time, and Message. The messages include status reports for encryption algorithms, database connections, firewall rules, LDAP configuration, client communication, server status, object cache, security warnings, and vault certificates.

Date	Time	Message
11/07/2023	03:33:19	ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA2-512 (Protocol Integrity), SHA2-512 (File Integrity)
11/07/2023	03:33:21	ITADM114I Successfully connected to Database, Database id 0.
11/07/2023	03:33:22	ITATS319W Firewall contains external rules.
11/07/2023	03:33:23	ITALD013I LDAP configuration refreshed successfully.
11/07/2023	03:33:41	ITAPW001I Firewall is open for client communication
11/07/2023	03:33:41	ITADB313I Server 12.6.0 (12.6.0.21) is up
11/07/2023	03:33:43	ITAQSO31I Object cache is loaded.
11/07/2023	03:33:43	ITATP151W Security warning - The Signature Hash Algorithm of the Vault certificate is SHA1. We recommend that you use at least Signature Hash Algorithm SHA256.
11/07/2023	03:33:43	ITATS319W Firewall contains external rules.
11/07/2023	03:48:51	ITATS319W Firewall contains external rules.
11/07/2023	04:03:54	ITATS319W Firewall contains external rules.
11/07/2023	04:18:57	ITATS319W Firewall contains external rules.
11/07/2023	04:18:59	ITATS319W Firewall contains external rules.

- The following lines are added to the dbparm.ini file located in the **C:\Program Files (x86)\Private Ark\Server\conf** directory:
 - **AllowNonStandardFWAddresses=[164.92.82.37],Yes,5000:outbound/tcp:** This is added to grant the necessary permissions for the HSM device.
 - **PKCS11ProviderPath="C:\ProCryptKM3000\lib\procryptoki.so":** This specifies the path to the HSM device's DLL file for its configuration.

```

30 EnablePreDefinedUsers=ALL
31 AutomaticallyAddBuiltInGroups="Backup Users,DR Users,Operators,Auditors,Notification Engines"
32 LicenseUsageAlertLevel=85,90,99
33 MaxTasksAllocation=8(CPM,AIMApp,AppPriv):7-23,16(CPM,AIMApp,AppPriv):23-7,1(PTAApp),1(PTAApp),1(PTAApp),1(PTAApp),1(PTAApp),1
34 ComponentNotificationThreshold=PIMProvider,Yes,30,1440;AppProvider,Yes,30,1440;OPMProvider,Yes,30,1440;CPM,Yes,720,1440;PVM
35 UserLockoutPeriodInMinutes=-1
36 MaskUserIsSuspendedMessage=No
37 AllowedVirusSafeFileTypes=DOC,DOT,XLS,XLT,EPS,BMP,GIF,TGA,TIF,TIFF,LOG,TXT,PAL,,
38 *AceServersIP=1.1.1.1,1.1.1.2
39 *AceServerPort=
40 TerminateOnDBErrorCodes=2003
41 AllowNonStandardFWAddresses=[164.92.82.37],Yes,5000:outbound/tcp
42 [BACKUP]
43 -BackupKey=C:\DemoOperatorKeys\Backup.key
44 [CRYPTO]
45 -SymCipherAlg=AES-256
46 -ASymCipherAlg=RSA-2048
47 [SYSLOG]
48 -UseLegacySyslogFormat=Yes
49 [HSM]
50 PKCS11ProviderPath="C:\ProCryptRM3000\lib\procryptoki.dll"
```

- The command **CAVaultManager SecureSecretFiles /SecretType HSM /Secret <hsmpincode>** is used to generate the **hsmpincode**

```
Administrator: Command Prompt
C:\Program Files (x86)\PrivateArk\Server>CAVaultManager SecureSecretFiles /SecretType HSM /Secret "procenne"
CLP0015: The option /SecretType is unknown
Usage: CAVaultManager <command> [command parameters]
If no command parameter is specified, you will be prompted for input.

C:\Program Files (x86)\PrivateArk\Server>CAVaultManager SecureSecretFiles /SecretType HSM /Secret "procenne"
ITA0B399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA2-512 (Protocol I
ntegrity), SHA2-512 (Files Integrity).
CAVLT146I HSM secret was secured successfully.

C:\Program Files (x86)\PrivateArk\Server>_
```

- This process adds the HSMPinCode line to the dbparm.ini file located in **C:\Program Files (x86)\Private Ark\Server\conf**

```

42 [BACKUP]
43 BackupKey=C:\DemoOperatorKeys\Backup.key
44 [CRYPTO]
45 SymCipherAlg=AES-256
46 ASymCipherAlg=RSA-2048
47 [SYSLOG]
48 UseLegacySyslogFormat=Yes
49 [HSM]
50 PKCS11ProviderPath="C:\ProCryptKM3000\lib\procryptoki.dll"
51 HSMPinCode=7F80BE725129E7C3696D546AFFD8A2A47CB97157067C261B83AC109041D91BC32C74FA2E7418A91C9EDB0DE6B207E2ED
52

```

- After this step, the command **CAVaultManager GenerateKeyOnHSM /ServerKey** is used to create the Secret (symmetric) key that will be used within the HSM device.

```

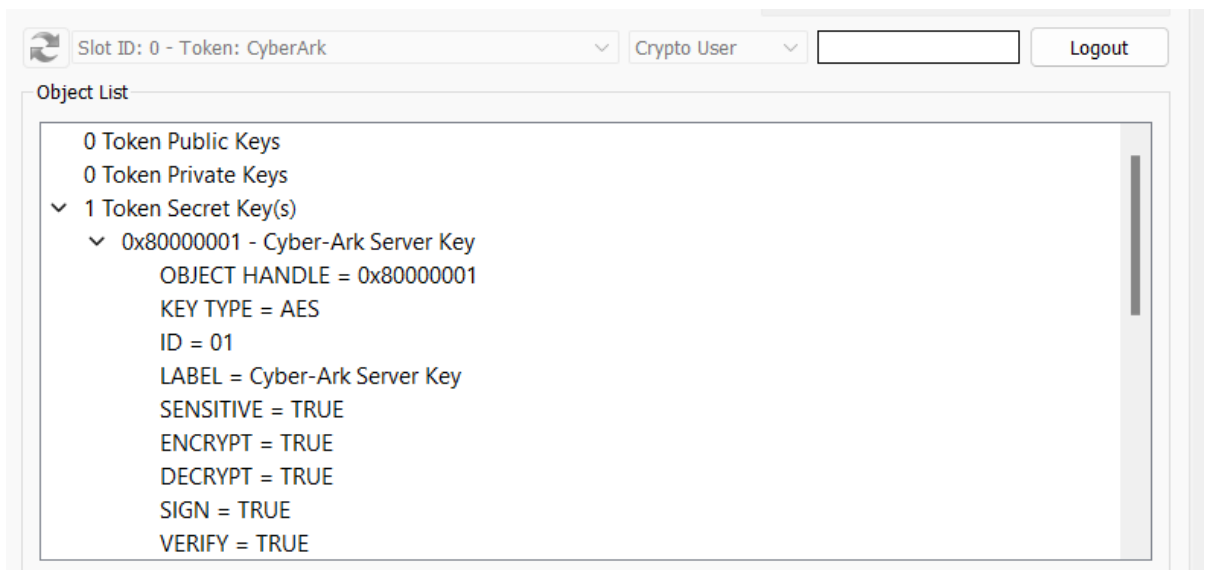
C:\Program Files (x86)\PrivateArk\Server>CAVaultManager SecureSecretFiles /SecretType HSM /Secret 1111
ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA2-512 (Protocol Integrity), SHA2-512
(Files Integrity).
CAVLT146I HSM secret was secured successfully.

C:\Program Files (x86)\PrivateArk\Server>CAVaultManager GenerateKeyOnHSM /ServerKey
ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA2-512 (Protocol Integrity), SHA2-512
(Files Integrity).
ITADM114I Successfully connected to Database, Database id 0.
2024-02-16 02:09:28.939 INFO [3796] [Procryptoki::Procryptoki@2223] Procryptoki v1.11.0
2024-02-16 02:09:28.940 INFO [3796] [ConfigFile::getConfigFileFullPath@446] Using config file: "C:\Program Files\Procenne\ProCrypt\etc\pro
ckrc"
2024-02-16 02:09:28.941 ERROR [3796] [Procryptoki::C_initialize@3223] Unable to parse config file: "C:\Program Files\Procenne\ProCrypt\etc\
prockrc"
2024-02-16 02:09:28.942 INFO [3796] [ConfigFile::getConfigFileFullPath@370] Using config file: "C:\Program Files\Procenne\ProCrypt\etc\con
fig"
2024-02-16 02:09:28.944 INFO [3796] [ConfigFile::getConfigFileFullPath@446] Using config file: "C:\Program Files\Procenne\ProCrypt\etc\pro
ckrc"
CAVLT187I Server Key was successfully generated on HSM device (KeyID=HSM#1).

C:\Program Files (x86)\PrivateArk\Server>

```

- As shown in the image, a symmetric key has been created within the HSM device. To verify the created key, it is checked using the ProcryptKeyManager tool.



- To use this key, the key replacement process is performed by following the instructions on the [CyberArk documentation website](#). For this purpose, the command ChangeServerKeys C:\DemoOperatorKeys C:\DemoOperatorKeys\VaultEmergency.pass HSM#4 is used.

```

Administrator: Command Prompt
03/12/2024 13:15:58 CHSRVK040I Changing keys for Safe PasswordManagerTemp.
03/12/2024 13:15:58 CHSRVK020I Keys of Safe PasswordManagerTemp changed successfully.
03/12/2024 13:15:58 CHSRVK040I Changing keys for Safe SCIM Config.
.....
03/12/2024 13:16:32 CHSRVK020I Keys of Safe SCIM Config changed successfully.
03/12/2024 13:16:32 CHSRVK040I Changing keys for Safe partner.
....
03/12/2024 13:16:32 CHSRVK020I Keys of Safe partner changed successfully.
03/12/2024 13:16:32 CHSRVK040I Changing keys for Safe Documentation and Resources.
....
03/12/2024 13:16:35 CHSRVK020I Keys of Safe Documentation and Resources changed successfully.
03/12/2024 13:16:35 CHSRVK040I Changing keys for Safe AppProviderCacheSafe.
....
03/12/2024 13:16:36 CHSRVK020I Keys of Safe AppProviderCacheSafe changed successfully.
03/12/2024 13:16:36 CHSRVK040I Changing keys for Safe ItamarSafe.
..
03/12/2024 13:16:36 CHSRVK020I Keys of Safe ItamarSafe changed successfully.
03/12/2024 13:16:36 CHSRVK040I Changing keys for Safe PasswordManager_Accounts.
..
03/12/2024 13:16:36 CHSRVK020I Keys of Safe PasswordManager_Accounts changed successfully.
03/12/2024 13:16:36 CHSRVK040I Changing keys for Safe OT.
..
03/12/2024 13:16:37 CHSRVK020I Keys of Safe OT changed successfully.
03/12/2024 13:16:37 CHSRVK054I ChangeServerKeys process was successful. DBParm.ini must be updated to point to new keys
for Vault to start.
03/12/2024 13:16:37 CHSRVK042I ChangeServerKeys process ended.

C:\Program Files (x86)\PrivateArk\Server>ChangeServerKeys.exe C:\DemoOperatorKeys C:\DemoOperatorKeys\VaultEmergency.pass HSM#4

```

- As shown in the image, the process has been successfully completed. Before starting the PrivateArk Server, the ServerKey parameter in the dbparm.ini file located in the C:\Program Files (x86)\PrivateArk\Server\Conf directory is updated.

```

C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log dbparm.ini
1 [MAIN]
2 TasksCount=20
3 DateFormat=DD.MM.YY
4 TimeFormat=HH:MM:SS
5 ResidentDelay=10
6 BasePort=1858
7 LogRetention=7
8 LockTimeOut=30
9 DaysForAutoClear=30
10 DaysForPicturesDistribution=Never
11 ClockSyncTolerance=600
12 TraceArchiveMaxSize=5120
13 VaultEventNotifications=NotifyOnNewRequest,NotifyOnRejectRequest,NotifyOnConfirmRequestByA
14 RecoveryPubKey=C:\DemoOperatorKeys\RecPub.key
15 ServerKey=HSM#4
16 StagingAreaDirectory=C:\PrivateArk\StagingArea
17 EntropyFile=C:\PrivateArk\Safes\entropy.rnd
18 DatabaseConnectionPasswordFile=C:\DemoOperatorKeys\VaultUser.pass
19 ServerCertificateFile=C:\DemoOperatorKeys\Server.pem
20 ServerPrivateKey=C:\DemoOperatorKeys\Server.pvk
MS ini file length: 2,191 lines: 53 Ln: 15 Col: 16 Pos: 415 Windows (CR LF) UTF-8 INS

```

- After saving the file, the PrivateArk Server is restarted.



The screenshot shows the 'Server Central Administration' window. The 'Messages' tab is selected, displaying a list of system messages. The messages are organized into three columns: Date, Time, and Message. The messages are dated 08/12/2024 and range from 23:00:49 to 23:01:00. The messages include status reports for encryption algorithms, database connections, LDAP configuration, firewall rules, and server status.

Date	Time	Message
08/12/2024	23:00:49	ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA2-512 (Protocol Integrity), SHA2-512 (Fi...
08/12/2024	23:00:53	ITADM114I Successfully connected to Database, Database id 0.
08/12/2024	23:00:53	ITATS319W Firewall contains external rules.
08/12/2024	23:00:54	ITALD013I LDAP configuration refreshed successfully.
08/12/2024	23:00:55	ITAFW001I Firewall is open for client communication
08/12/2024	23:00:55	ITAFW052I Firewall is open for non standard address.
08/12/2024	23:00:55	ITADB313I Server 12.6.0 (12.6.0.21) is up
08/12/2024	23:00:57	ITAQSO31I Object cache is loaded.
08/12/2024	23:01:00	ITATP151W Security warning - The Signature Hash Algorithm of the Vault certificate is SHA1. We recommend that you use at least Signature Has...
08/12/2024	23:01:00	ITATS319W Firewall contains external rules.

REFERENCES

- <https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/10.10/en/Content/PAS%20INST/configuring-HSM-Key-Management.htm?Highlight=hsm>
- <https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.1/en/Content/PASIMP/Configuring-HSM-Key-Management-in-a-DV-Vault-environment.htm>