CyberArk Vault

v14.2.1

Integration Guide

SecurityServer

6.1.1

utimaco®

Imprint

Copyright 2025	Utimaco IS GmbH
	Germanusstr. 4
	D-52080 Aachen
	Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226)
	EMEA +49 800-627-3081
	APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2025-08-06
Status	PUBLISHED
Document No.	IG-2025-0035

Table of Contents

1 Introduction

This guide is part of the information and support provided by Utimaco. Additional documentation produced to support your Utimaco SecurityServer product can be found in the document directory of the Utimaco SecurityServer product bundle.

All Utimaco SecurityServer product documentation is available from Utimaco's website at https://utimaco.com/.

1.1 About This Guide

This guide explains how to integrate an Utimaco CryptoServer Hardware Security Module (HSM) with CyberArk Vault. Utimaco securely generates and stores the private keys of the server keys used by CyberArk Vault.

1.2 Target Audience

This guide is intended for administrators of CyberArk Vault and Utimaco HSMs.

1.3 Purpose of this Integration

This integration ensures that privileged passwords are safe, automatically managed, and used securely, reducing risks and meeting compliance needs.

1.4 Abbreviations

Abbreviations	Meaning
CA	Certificate Authority
CMD	Command prompt
CSAR	Cloud Service Architecture
DB	Database

Abbreviations	Meaning
DLL	Dynamic Link Library
GUI	Graphical User Interface
HSM	Hardware Security Module
IP	Internet Protocol
LAN	Local Area Network
MBK	Master Backup Key
PCIe	PCI Express Interface
PIN	Personal Identification number
PKCS#11	Public-Key Cryptography Standard #11
SO	Security Officer
URL	Uniform Resource Locator

Table 1: List of Abbreviations

1.5 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press the **OK** button.
`Monospaced`	File names, folder and directory names, commands, file outputs, programming code samples	You will find the file `example.conf` in the `/exmp/demo/` directory.
Italic	References and important terms	See Chapter 3, "Sample Chapter", in the *CryptoServer - csadm Manual* or [CSADMIN].

Table 2: Document conventions

Special icons are used to highlight the most important notes and information.

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

This message marks the result expected after the successful execution of an instruction.

2 Product Overview

2.1 CyberArk Vault

At the core of the CyberArk Privileged Access Manager Solution is the CyberArk Digital Vault, which contains a highly secure database that stores privileged-account credentials, access-control policies, credential management policies, and audit information. To protect both the Digital Vault database itself and the data stored within the database, CyberArk uses a multi-layered encryption hierarchy.

Each individual file and safe within the Digital Vault database are uniquely encrypted using a randomly generated encryption key. At the top of the key hierarchy, CyberArk utilizes a unique server key and a unique recovery key. The server key is required to start the Digital Vault, and in accordance with the CyberArk Digital Vault Security Standard, this encryption key is stored within a Utimaco hardware security module (HSM).

2.2 Utimaco SecurityServer HSM

SecurityServer is a hardware security module developed by Utimaco IS GmbH. SecurityServer is a physically protected specialized computer unit designed to perform sensitive cryptographic tasks and to securely manage – as well as store – cryptographic keys and data. It can be used as a universal, independent security component for heterogeneous computer systems.

3 Integration Requirements and Prerequisites

Ensure that the system environment you will be using meets the following hardware and software requirements.

3.1 Tested Versions

The following integrations have been successfully tested with the Utimaco HSM and the CyberArk Vault.

Operating System	CyberArk Vault Version	Utimaco Security Server Version	Utimaco HSM
Windows Server 2019	v14.2.1	SecurityServer 6.1.1	CryptoServer CSe-Series/Se-Series

Table 3: List of Tested Versions

3.2 Software Requirements

Software	Software Requirements
HSM Utility	PKCS#11 Tool Version 2 (p11tool2)
HSM Interfaces	SecurityServer PKCS#11 Provider

Table 4: List of Software Requirements

3.3 Hardware Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	CryptoServer CSe-Series/Se-Series LAN with firmware SecurityServer 6.1.1 or higher
Utimaco PCI-e HSM	CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 6.1.1 or higher

Table 5: List of Hardware Requirements

Set up an account on the Utimaco support portal and request download access at the following URL: https://support.hsm.utimaco.com/.

3.4 Prerequisites

Before you begin, please ensure that you have:

- The Utimaco CryptoServer HSM set up and configured. Refer to the CryptoServer documentation to set up the HSM.
- The MBK created and stored on each HSM. Refer to the CryptoServer documentation to set up the MBK.
- The CryptoServer Default Admin replaced with a new admin user.
- An operating system listed in Tested Versions.
- SecurityServer listed in Tested Versions.
- The PKCS#11 library set up and configured as per your environment. Refer to the CryptoServer documentation to set up and configure the PKCS#11 library.
- A user with Administrative privileges, which is required to install the software.
- Downloaded and installed CyberArk Vault. Refer to the steps in the CyberArk Vault Documentation page.

The steps for installing CyberArk Vault are outside the scope of this document. Please follow the above links for more information about CyberArk Vault installation and configuration.

4 Installing and Configuring Utimaco SecurityServer Software

4.1 Download and Install Utimaco Software

If you have not already done so, please create and request an Utimaco Support Portal Account. This will allow you to download the software components needed for this installation.

If you have purchased an HSM from Utimaco, locate the included product bundle that contains the Windows software packages.

Install the latest version of the SecurityServer software as described in the SecurityServer manual for the HSM. We recommend that you uninstall any SecurityServer software before installing the new software.

4.2 Update cs_pkcs11_R3.cfg

On Windows, as part of CryptoServer software installation, cs_pkcs11_R3.cfg will be automatically created and available under the “C:\ProgramData\Utimaco\PKCS11_R3” folder.

cs_pkcs11_R3.cfg

```
[Global]
# For windows:
Logpath = C:/ProgramData/Utimaco/PKCS11_R3
# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)
Logging = 1
# Prevents expiring session after inactivity of 15 minutes KeepAlive = true
# Set the Device to connect with [CryptoServer]
# Device specifier Device = <HSM_IP>
```

For more information regarding the commands and command parameters, please check the Utimaco CryptoServer documentation. The device may be a CryptoServer (PCIe or LAN) device. The device line will follow one of these patterns, based on the HSM form-factor:

`Device = 288@<HSM IP address> Hardware (LAN) HSM` OR

`Device = /dev/cs2.0 Hardware (PCIe) HSM`

To make your testing easier, enable the PKCS#11 log file. You can enable it by editing the Logging Loglevel. Set the LogPath and Logging Loglevel to 1. For testing, you may want to increase them to 4.

The added LogPath points to a writable directory, not to a file.

If you encounter problems, check the log file named `cs_pkcs11_R3.log` in the LogPath-defined directory. When you are done testing, change the Logging to 1 or 2. This will limit the logging to only critical and important messages.

4.3 Create SO User and Initialize a Slot

You must initialize a slot with a custom label using p11tool2.

First, using `p11tool2`, create the SO or Security Officer. Then, using a `p11tool2` command, initialize the Slot that you want to use and the slot user, as shown below.

›_ Console

```
# p11tool2 slot=<slot_no.> Label=<token_label> Login=ADMIN,<ADMIN.key>

InitToken=ask

# p11tool2 slot=<slot_no.> LoginSO=ask SetPin=ask,ask # p11tool2 slot=<slot_no.>
LoginSO=ask InitPIN=ask

# p11tool2 slot=<slot_no.> LoginUser=ask SetPIN=ask,ask
```

```
C:\Program Files\Utimaco\SecurityServer\Administration>p11tool2 slot=0 Label=Cyb
erArkVault Login=ADMIN,ADMIN_SIM.key InitToken=ask
Enter SO PIN:
Repeat SO PIN:
```

Figure 1 : Slot Initialization Output

5 Integrating CyberArk Vault with Utimaco HSM

5.1 Configure CyberArk Vault to Use Utimaco HSM

1. To allow communication between Vault Server and Utimaco HSM, open the CyberArk Vault configuration file located at `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparam.ini` and configure the `AllowNonStandardFWAddresses` parameter to open the Firewall and enable access to the HSM.


dbparam.ini

```
AllowNonStandardFWAddresses=[HSM-IP],Yes,288:inbound/tcp,288:outbound/tcp
```


Replace HSM IP and port according to your setup.

2. Specify Utimaco `PKCS#11` provider DLL in the PKCS11ProviderPath parameter in the `DBParm.ini` file.


dbparam.ini

```
PKCS11ProviderPath=C:\Program Files\Utimaco\SecurityServeer\Lib\cs_pkcs11_R3.dll
```

3. Save the changes to the dbparam.ini file and close it.
4. Restart the PrivateArk Server service.

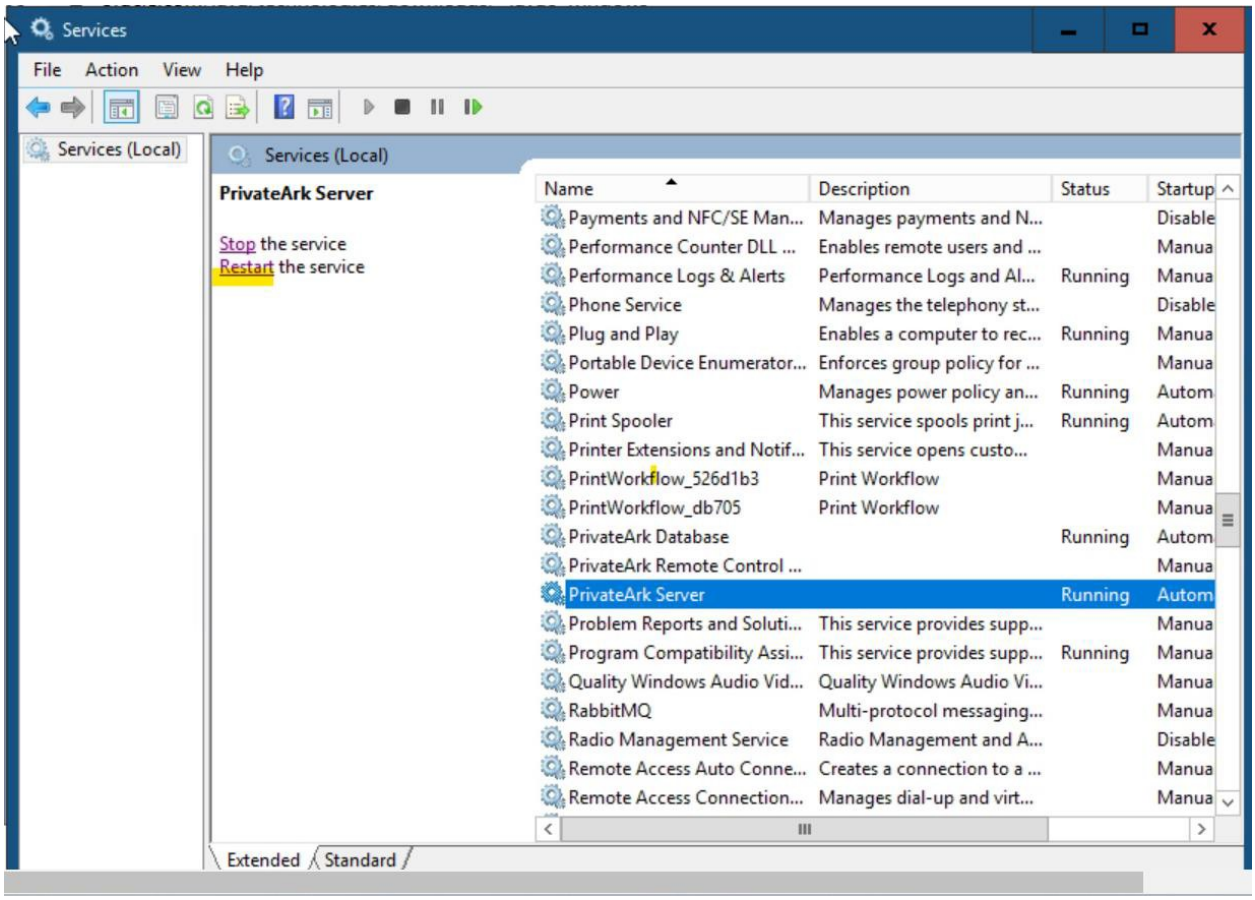


Figure 2 : Restart PrivateArk Server Service

5. Store the HSM Slot PIN as an encrypted password to access the Utimaco HSM:

```
›_ Console
```

```
CAVaultManager.exe SecureSecretFiles /SecretType HSM /Secret 12345678
```

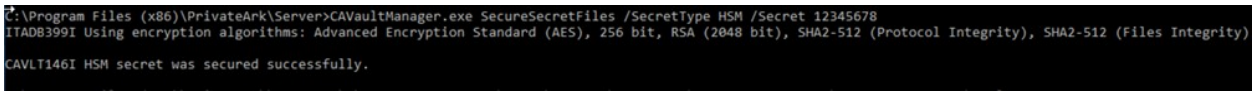


Figure 3 : CAVaultManager SecureSecretFiles command output

6. Replace 12345678 with the Slot PIN.

7. Open the `DBParm.ini` file and verify that the **HSMPinCode** parameter has been added with the encrypted value of the Slot PIN.

dbparam.ini

```
HSMPinCode=2F3C61B954886FAA08EFFCE92137981A8B2E3459A58D8571CB262FCA8E8E8C92EA7 9E24A12BFA30E4FDFB8E0698D6D63
```

5.2 Generating the Vault's Server Key on the Utimaco HSM

In the most secure CyberArk Vault setup, the Server key is directly generated in the secure environment of the HSM. After the initial vault configuration is complete, you can proceed and generate the Vault Server key on the HSM. Once this process is complete, the server key is stored as a non-exportable key on the HSM PKCS#11 slot and is used by the vault.

1. Stop the PrivateArk Server service.

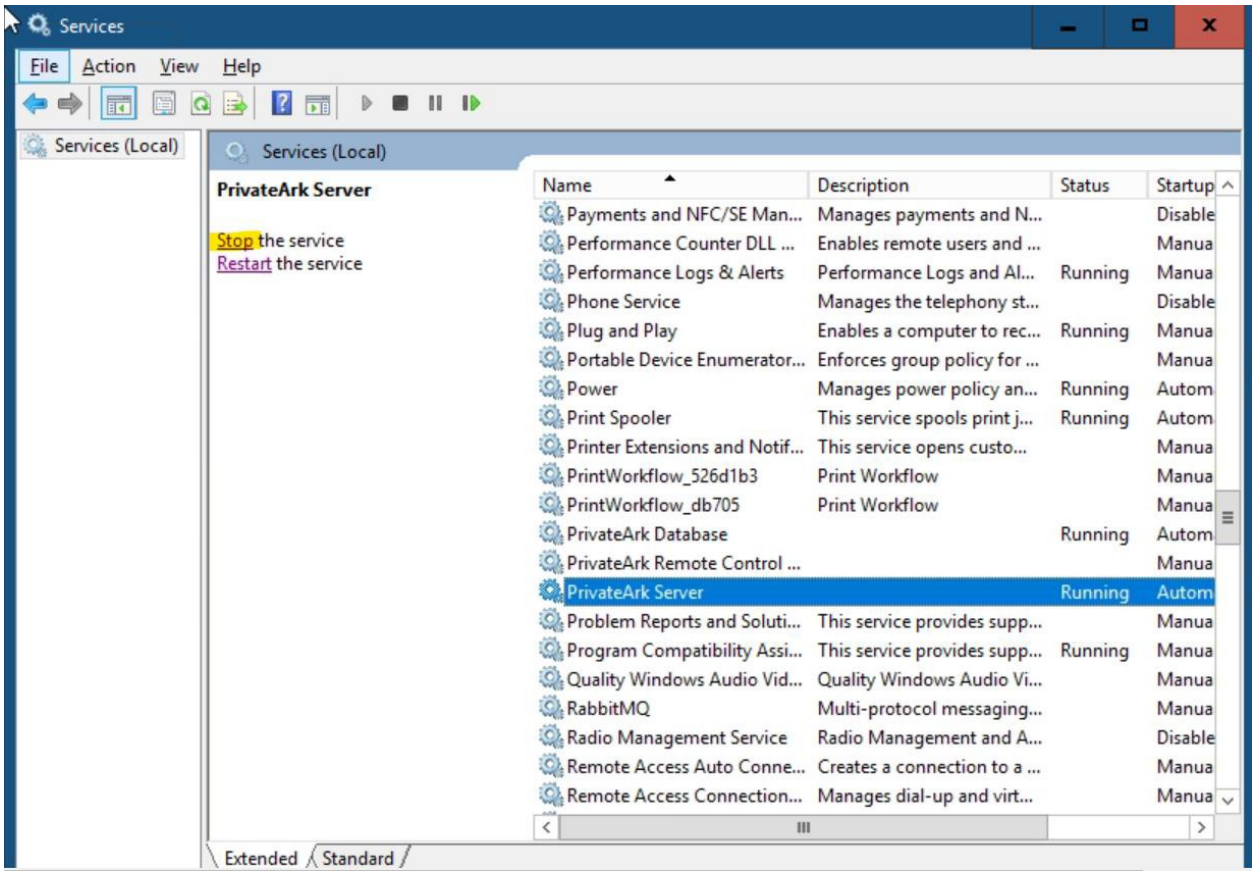


Figure 4 : Stop the PrivateArk Server Service

2. Open `cmd` as administrator.

3. Run the `GenerateKeyOnHSM` command to generate a new server key using `CAVaultManager`. Make sure that the result confirms that the server key was successfully generated on the HSM. You should see the following response:

```
›_ Console
```

```
CAVaultManager.exe GenerateKeyOnHSM /ServerKey
```

Figure 5 : Generate server key on Utimaco HSM

The above command generates a new key for the Vault server, stores it in the previously initialized `HSM PKCS#11` slot, and returns the keyID.

4. Note down the HSM key generation number returned in the `CAVLT187I log (KeyID=HSM#X)`.
5. Verify that the key has been generated on the HSM with the `p11tool2` command.

›_ Console

```
P11tool2 slot=0 LoginUser=ask ListObjects
```

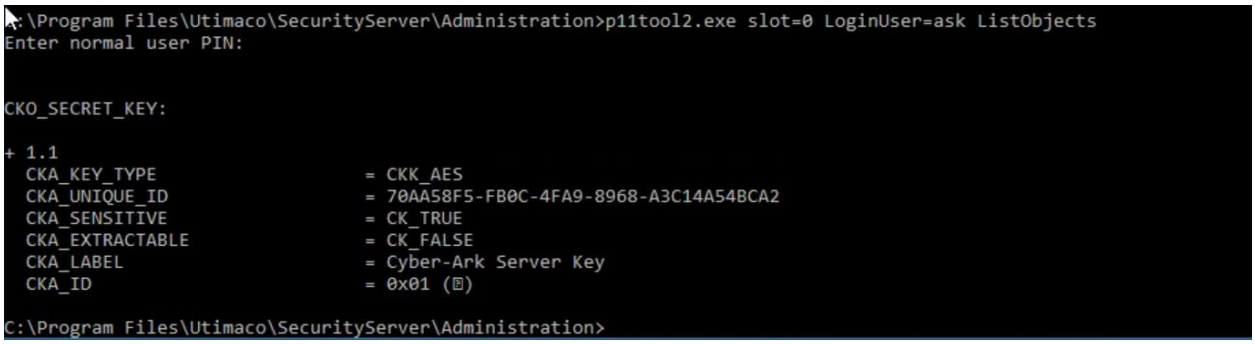


Figure 6 : Key List

6. Mount the recovery private key (`recprv.key`) to the Vault server.
7. Open the `DBParm.ini` file located at `C:\Program Files (x86)\PrivateArk\Server\Conf\dbparam.ini.`
8. Set the RecoveryPrvKey parameter to the recovery private key path location and save the file.

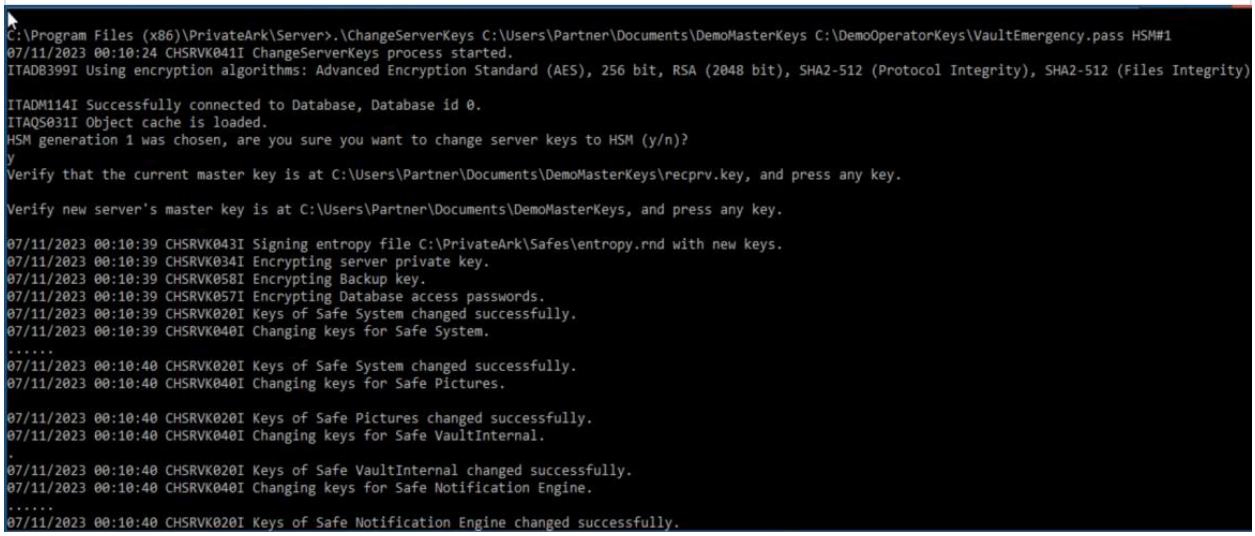
dbparam.ini

```
RecoveryPrvKey=<path_to_recovery_private_key>recprv.key
```

9. Navigate to the `C:\Program Files (x86)\PrivateArk\Server folder`, then open `cmd` as an administrator.
10. Change the existing server key to use the newly generated one on the Utimaco HSM.

›_ Console

```
ChangeServerKeys.exe <path_to_keys directory> <path_to_VaultEmergency.pass>
HSM#<keyID_no.>
For example:
ChangeServerKeys.exe C:\Users\Partner\Document\DemoMAsterKeys C:
\DemoOperatorKeys\VaultEmergency.pass HSM#1
```



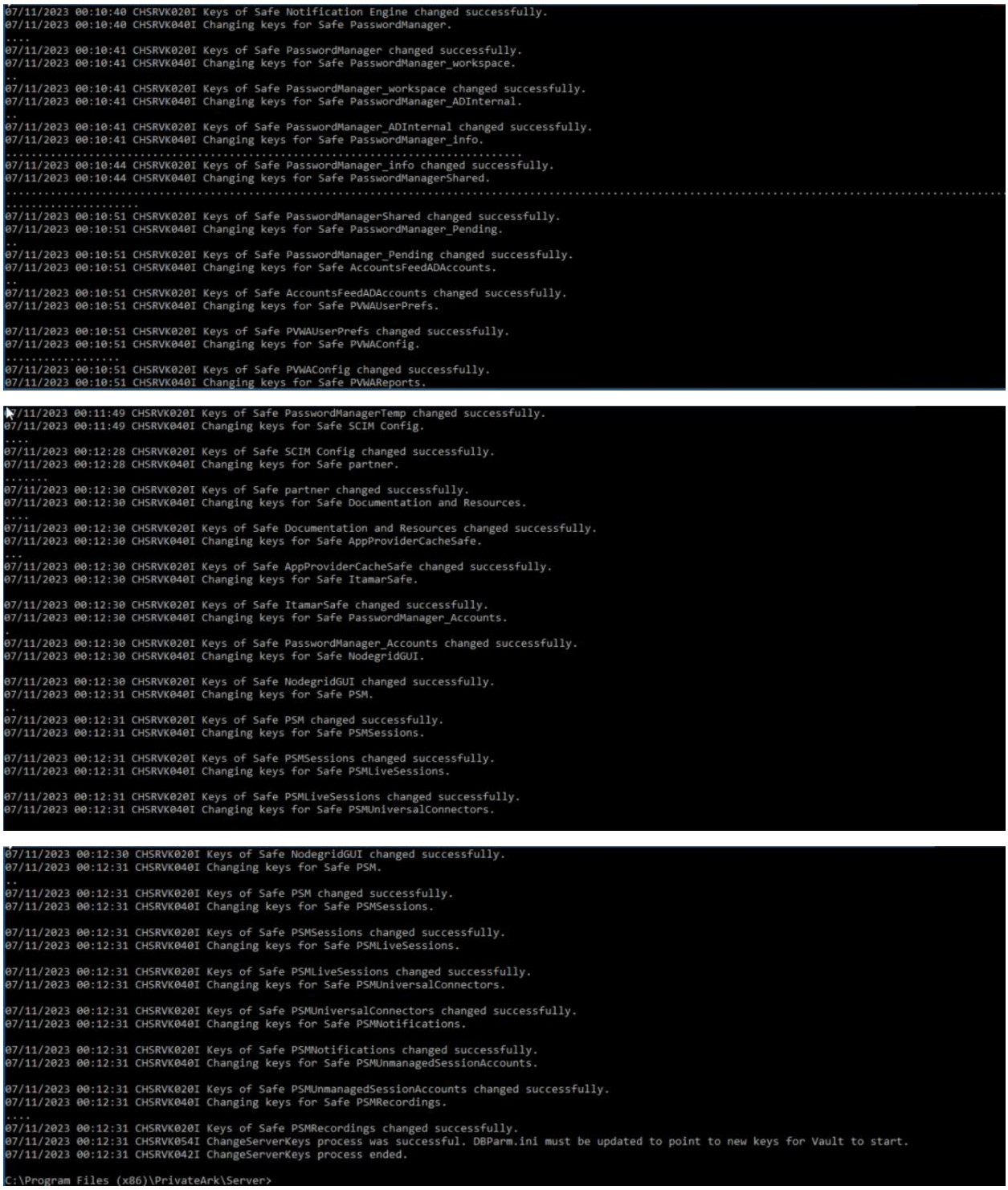


Figure 7 : ChangeServerkey to HSM output

11. Make sure that the result confirms that the Change Server keys process was successful.

12. Open the `DBParm.ini` and change the `ServerKey=HSM#X` parameter. Replace X with the HSM key generation number.

dbparam.ini

```
ServerKey=HSM#1
```

13. Save the file.
14. Start the PrivateArk Server service and ensure that no errors are printed to the console.
15. Verify that you can log on to the Vault using CyberArk authentication.

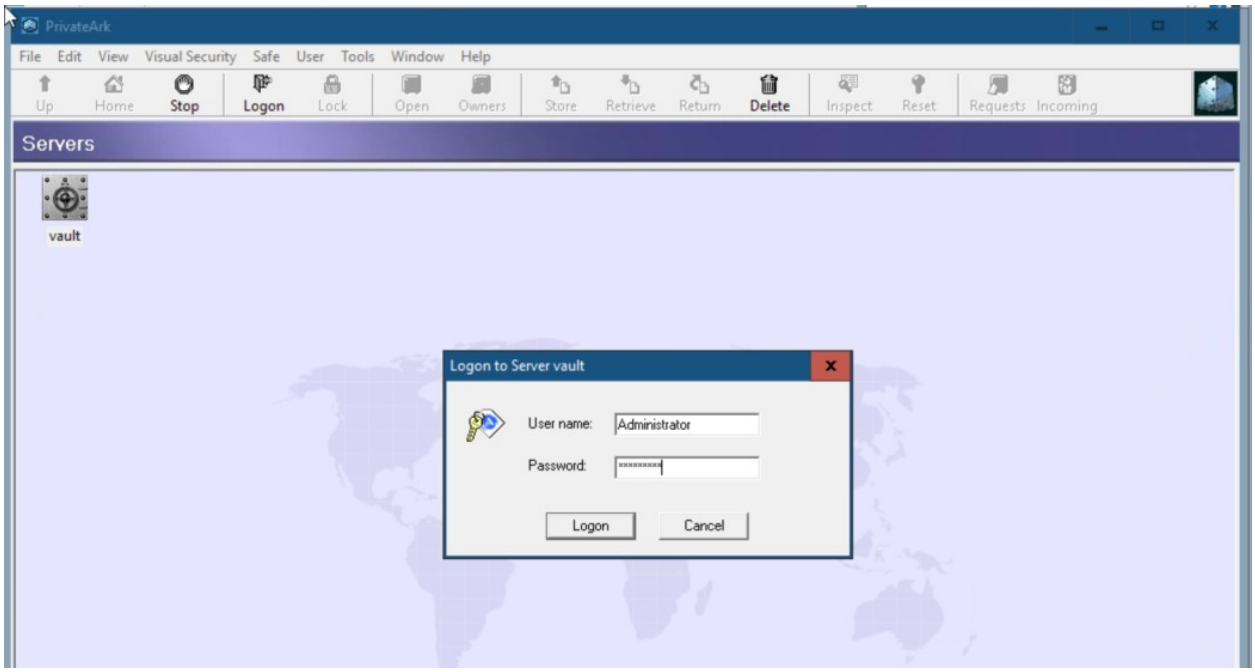


Figure 8 : Logon to Vault using CyberArk authentication

16. Unmount the recovery private key from **dbparm** (revert to default value: `d:\recprv.key`).

5.3 Migrate Existing Server Key to HSM

To migrate the existing server key to Utimaco HSM:

1. Complete the steps given in 5.1 Configure CyberArk Vault to use Utimaco HSM.
2. Stop the **PrivateArk** Server service.

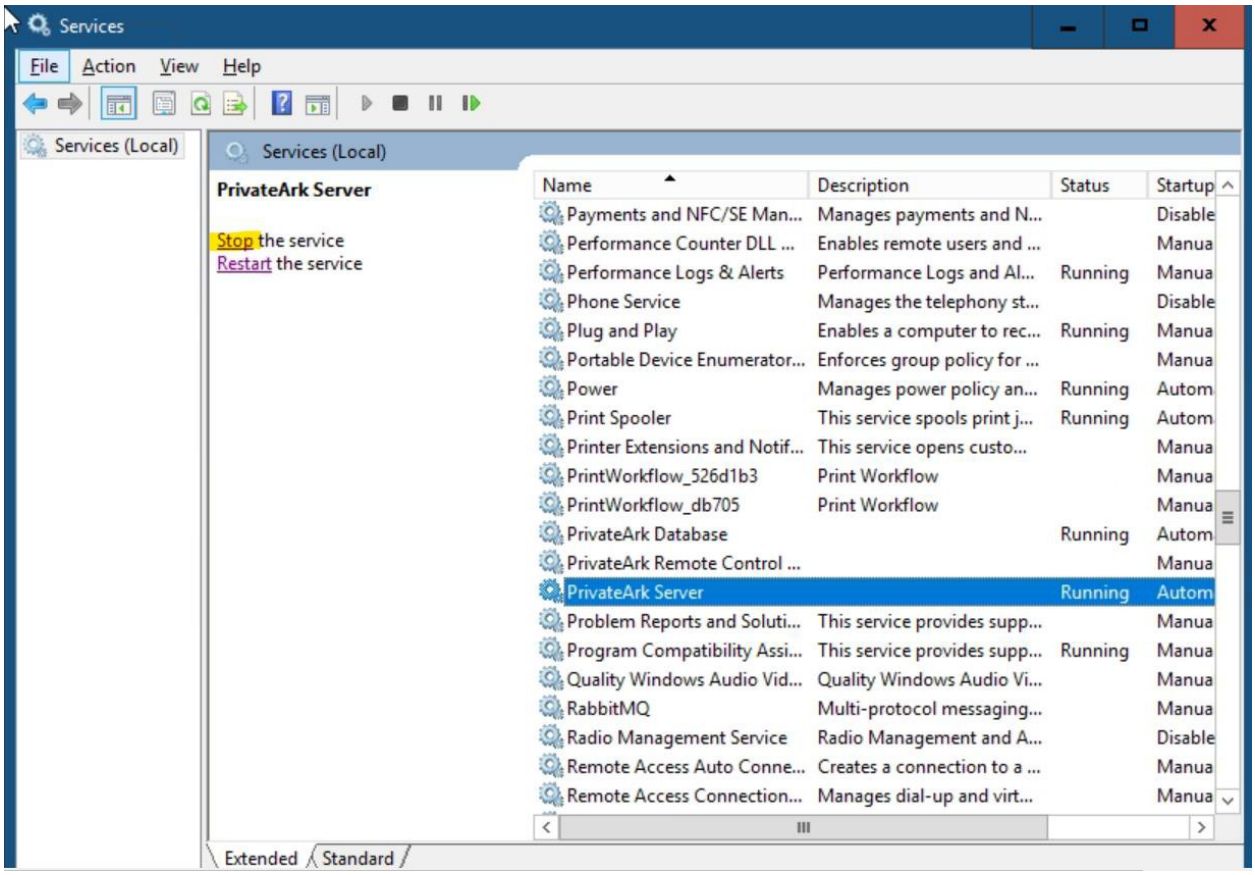


Figure 9 : Stop services of PrivateArk Server

3. Navigate to the `C:\Program Files (x86)\PrivateArk\Server` folder, then open cmd as administrator.
4. Using `CAVaultManager`, run the `LoadServerKeyToHSM` command to upload the server key to store in the Utimaco HSM.

```
›_ Console
```

```
CAVaultManager.exe LoadServerKeyToHSM /WrapKey
```

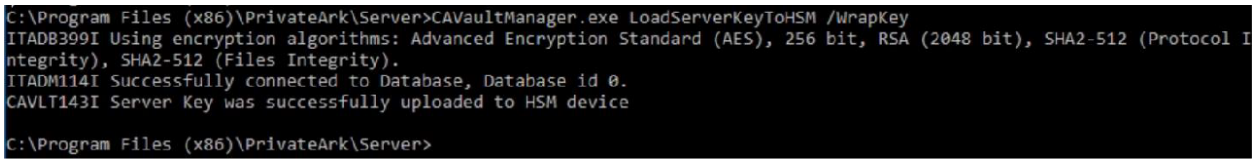


Figure 10 : Migrate Server Key to HSM

Ensure that the result confirms that the server key has been uploaded to the HSM:

1. Verify that the keys have been uploaded to Utimaco HSM using `p11tool2`.

›_ Console

```
p11tool2 slot=0 LoginUser=ask ListObjects
```

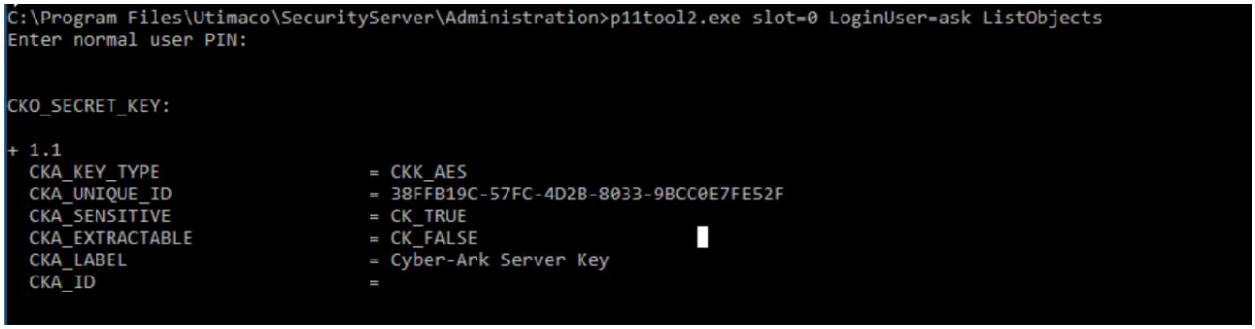


Figure 11 : Key list

2. Open the `DBParm.ini` file located at `C:\Program Files (x86)\PrivateArk\Server\Conf`.
3. Set the `ServerKey=HSM` parameter.

dbparam.ini

```
ServerKey=HSM
```

4. Save the file.
5. Start the **PrivateArk** Server service and verify that there are no errors in the console.
6. Verify that you can log on to the Vault using CyberArk authentication.

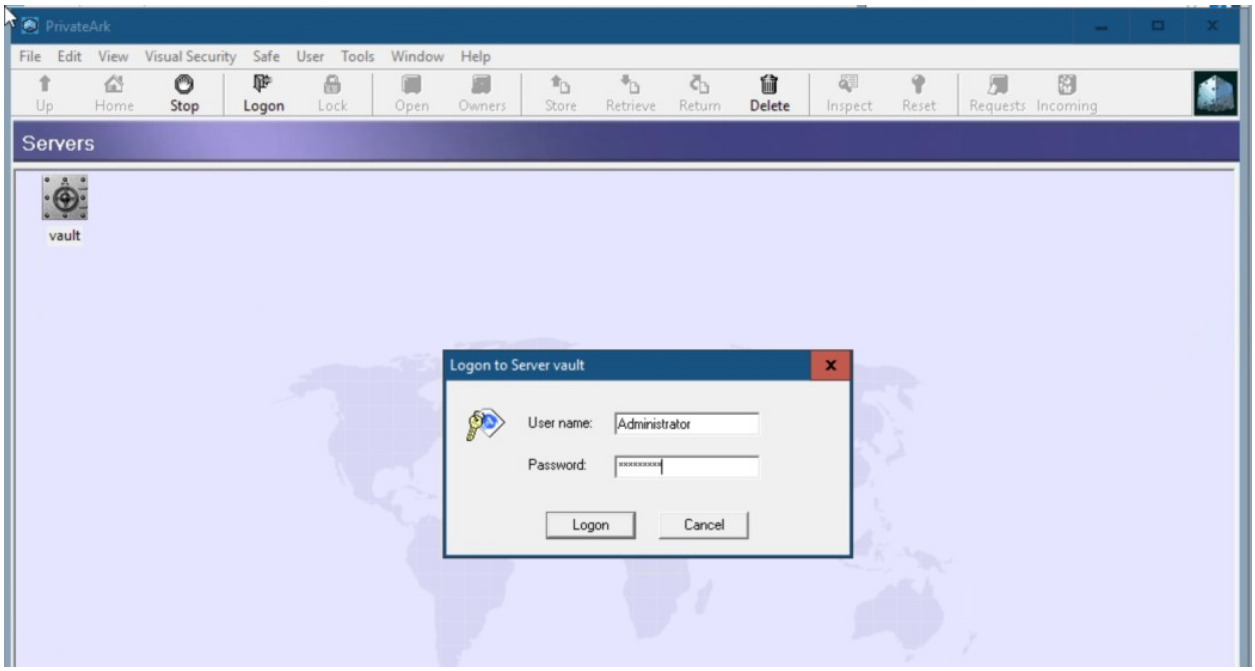


Figure 12 : Logon to Vault using CyberArk authentication

This completes the integration for CyberArk Vault with Utimaco SecurityServer.

6 Troubleshooting

Error	Diagnosis
Unable to create server key	Create the correct HSM secret PIN, stop the Vault service, and then try to create the server key again on the HSM.
Unhandled Exception: System.AccessViolationException: Attempted to read or write protected memory. This is often an indication that other memory is corrupt. at mainCRTStartup()	Make an appropriate entry for the ServerKey parameter in the `dbparam.ini` file.

Table 6: List of Errors and their Diagnoses

7 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Germanusstr. 4
52080 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.

8 Further Information

This document forms part of the information and support provided by Utimaco IS GmbH. Additional documentation can be found on the product CD in the Documentation directory.

All CryptoServer product documentation is also available at the Utimaco IS GmbH website: https://utimaco.com/.

9 References

Reference	Title/Company	Document No
[CSADMIN]	CryptoServer – csadm Manual/Utimaco IS GmbH	2009-0003
[CSTrSh]	CryptoServer Troubleshooting/Utimaco IS GmbH	M011-0008-en
[CSADMIN2]	CryptoServer_csadm_Manual_Systemadministrators.pdf	2009-0003
[CSP11Tool2]	CryptoServer_p11tool2_Manual.pdf	2012-0004
[CSPKCSM]	CryptoServer - PKCS#11 P11CAT Manual	M013-0001-en
[CSLAN5]	CryptoServerLAN_Manual_Systemadministrators.pdf	2018-0004

Table 7: References