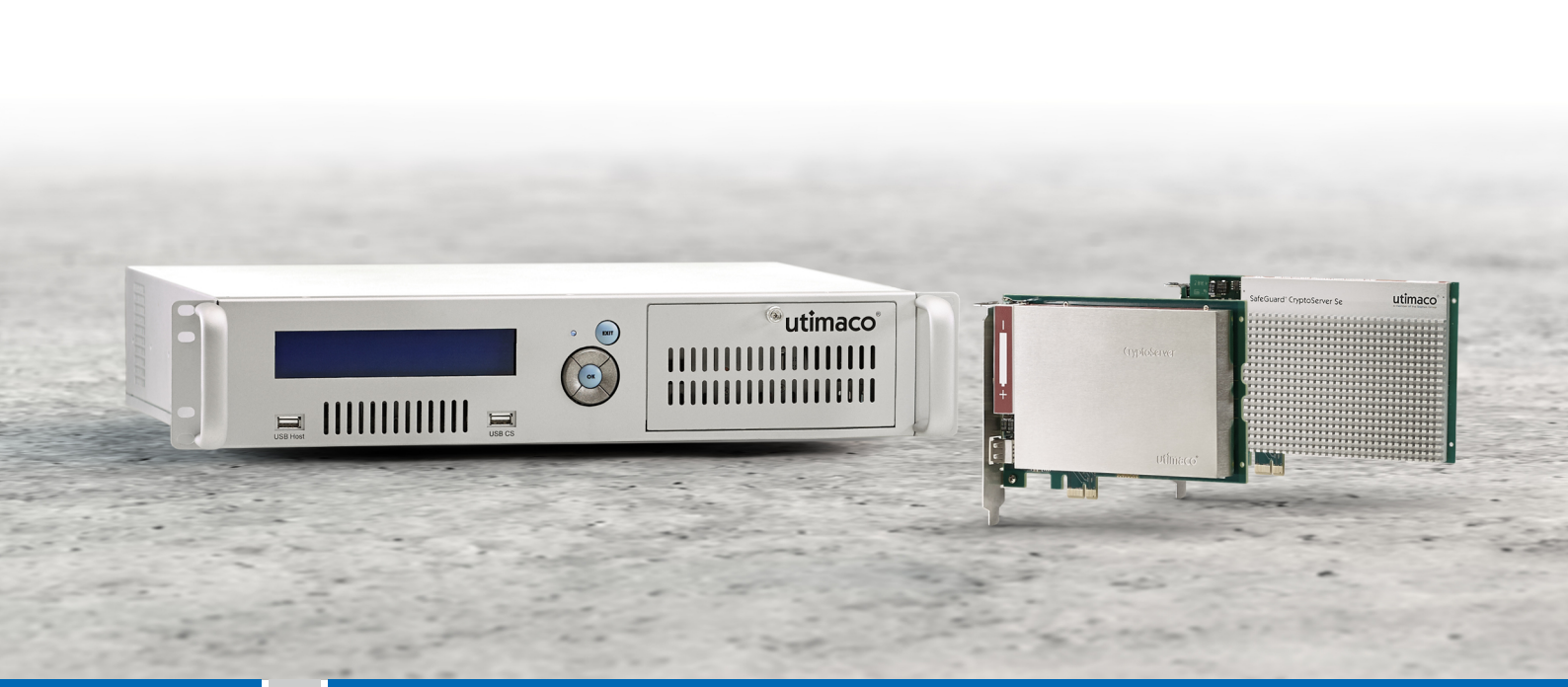


Integration Guide

CyberArk
Microsoft Windows

utimaco®

Imprint

copyright 2016	Utimaco IS GmbH Germanusstrasse 4 D-52080 Aachen Germany
phone	+49 (0)241 / 1696-200
fax	+49 (0)241 / 1696-199
web	http://hsm.utimaco.com
email	support-cs@utimaco.com
document version	1.0.4
date	April 2016
author	M. Sc. Ariano-Tim Donda
document no.	IG_CyberArk

Contents

1 Introduction **4**

2 Overview **4**

3 Requirements **5**

4 Components **5**

5 HSM Configuration **6**

5.1 HSM Host Software Installation 6

5.2 HSM Initialization 7

6 Installation of CyberArk **8**

6.1 Initial Vault Configuration 8

6.2 Loading the Server Key into the HSM 9

6.3 Generating the Server Key in the HSM 9

7 Further Information **11**

1 Introduction

The Utimaco CryptoServer is a hardware security module developed by Utimaco, i.e. a physically protected specialized computer unit designed to perform sensitive cryptographic tasks and to securely manage cryptographic keys and data. In a Utimaco CryptoServer security system security-relevant actions can be executed and security relevant information can be stored. It can be used as a universal, independent security component for heterogeneous computer systems.

2 Overview

The Privileged Identity Management (PIM) Suite of CyberArk is a full life-cycle solution for managing privileged accounts inside an enterprise environment. At the very heart of this Suite lies the Enterprise Password Vault (EPV) which enables organizations to secure, manage and log all activities associated to privileged passwords. In order to further raise the security of the password management solution EPV offers a PKCS#11 hardware interface which enables the integration of an HSM in the role of the security anchor in the infrastructure. Introducing a FIPS 140-2 certified HSM into an identity management solution maximizes the security of the complete infrastructure and demonstrates that proper due care measures have been taken to ensure confidentiality, integrity and availability of critical enterprise data.

3 Requirements

Please ensure that you have a copy of the CryptoServer Manual for System Administrators available. The present integration guide also assumes that a Microsoft Server 2008 R2 SP1 EN has already been installed. Please contact your CyberArk support representative in case you intend to use another installation platform.

Software- and Hardware Requirements

HSM Model	CryptoServer CS(e)-Series/Se-Series/Se-Gen2-Series PCI(e) CryptoServer CS(e)-Series/Se-Series/Se-Gen2-Series LAN CryptoServer Simulator
HSM Firmware	SecurityServer 4.0.0
Software	SecurityServer 4.0.0 Windows Server 2008 R2 SP1 EN

4 Components

In this section we give a quick overview of the components required for setting up a CyberArk EPV and integrating a CryptoServer HSM into your identity management infrastructure. The CyberArk Server and Administrative Client have been installed on the same machine for this guide. Further on the PKCS#11R2 interface and administrative tools of Utimaco have also to be installed on the same machine. Last but not least, a Java run-time environment together with the corresponding Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy files have to be installed on the same machine. Detailed installation and configuration instructions are provided in the following two sections.

5 HSM Configuration

5.1 HSM Host Software Installation

After installing the administrative and PKCS#11R2 components from the SecurityServer 3.20.0 Utimaco Product CD, following steps must be taken:

- Copy the 32bit variant of the PKCS#11R2 library (cs_pkcs11_R2.lib) out of the SecurityServer 3.20.0 product CD into your SysWOW64 directory.
- Copy the 64bit variant of the PKCS#11R2 library (cs_pkcs11_R2.lib) out of the SecurityServer 3.20.0 product CD into your System32 directory.
- Verify that a system variable named: CS_PKCS11_R2_CFG is pointing to your PKCS#11R2 configuration file (cs_pkcs11_R2.cfg). This variable is automaticaly created if you follow the SecurityServer 3.20.0 installation wizard. If the wizard was not used the variable has to be created manualy.
- In the cs_pkcs11_R2.cfg configuration file make sure that the parameter `KeepAlive` is set to `true` otherwise your PKCS#11 session between CyberArk Vault and HSM will be terminated after 15 minutes of being idle resulting in the necessity to re-authenticate the Vault Server towards the HSM every time it is used.

5.2 HSM Initialization

In order to interface CyberArk EPV to a Utimaco CryptoServer HSM you need to initialise a PKCS#11R2 slot with a security officer (SO) and a PKCS#11 cryptographic user (USER) role in advance. The credential used to log on to the PKCS#11 slot will later on be used from the CybeArk EPV to authenticate against the HSM and store/generate the CyberArk Server Key. To configure a PKCS#11R2 slot (slot#0 in this case) do the following:

- By using Utimaco's PKCS#11R2 command line tool (p11tool2) logon to the HSM as a user with user management rights and initialise the PKCS#11 SO role:

```
CONSOLE
p11tool2 slot=0 Login=ADMIN,:cs2:cyb:USB0 Label=CyberArkEPV
         InitToken=123456
```

- After the SO has been initialised, you have to authenticate the SO to be able to initialise the PKCS#11R2 cryptographic user:

```
CONSOLE
p11tool2 slot=0 LoginSO=123456 InitPin=654321
```

This finishes the configuration of the PKCS#11R2 slot #0 on the HSM. The PIN used for the PKCS#11 user will be used during the configuration of CyberArk EPV to access the CyberArk Server key.

6 Installation of CyberArk

An HSM can be integrated into the CyberArk suite in two ways. Either by loading an existing CyberArk Server Key into the PKCS#11 slot or, in the more secure setup, by generating it directly inside the secure HSM environment. Both integration paths are described in the following two subsections. The installation of CyberArk EPV is described in detail in the CyberArk suite's installation guide. Assuming that the installation of the CyberArk Server Service has been successful the next step is to configure the HSM key management in order to store your critical CyberArk Server Key as non exportable key on the HSM.

If your vault is already installed the following services may need to be enabled and started for the installation *Windows installer*, *Windows Modules installer* and *Windows Update*. These services should be stopped and disabled once the HSM software is successfully installed.

6.1 Initial Vault Configuration

1. For interfacing a CryptoServer LAN HSM the Firewall has to be configured to allow communication to the HSM. In the DBParm.ini configure the `AllowNonStandardFWAddresses` parameter to open the Firewall and enable access to the HSM.
   ```
   AllowNonStandardFWAddresses=[HSM-IP],Yes,288:inbound/tcp,288:outbound/tcp
   ```
2. As a next step the PKCS#11 provider DLL has to be specified. This is done by entering the parameter `PKCS11ProviderPath` into DBParm.ini and pointing it to the 64bit PKCS#11R2 DLL located in the directory System32.
   ```
   PKCS11ProviderPath=C:\Windows\System32
   ```
3. Save and close the DBParm.ini configuration file.
4. Encrypt the PKCS#11R2 Slot user PIN used for accessing the PKCS#11 Slot on the HSM by running CyberArk's command line tool `CAVaultManager` with following arguments:
   ```
   CAVaultManager SecureSecretFiles /SecretType HSM /Secret <PKCS#11R2_USER_PIN>
   ```
5. Open the DBParm.ini file and verify that the `HSMPinCode` parameter has been added with the encrypted value of the PIN code.
6. Restart the CyberArk Server Service in order for the new Firewall rules to be effective.

7. Shutdown the PrivateArk Server Service.

6.2 Loading the Server Key into the HSM

When the initial vault configuration is done we can proceed and store the PrivateArk Server Service key on the HSM. Once this process is through, the server key is stored as a non exportable key on the HSM PKCS#11 slot and can be used by the vault.

1. Verify that the PrivateArk Server Service is not running.
2. With the help of CyberArk's command line tool CAVaultManager run the following command:

```
CONSOLE

CAVaultManager LoadServerKeyToHSM
```

3. Verify that the load operation successfully confirms.
4. Open DBParm.ini and change the `ServerKey` parameter value to:
   `ServerKey=HSM`
5. Start CyberArk's Server Service and verify that you can log on to the Vault.

With the above described procedure you have successfully imported the PrivateArk Server Service Key into the PKCS#11 slot on the HSM and can proceed with the installation of of the admin client as described in CyberArk's installation guide.

6.3 Generating the Server Key in the HSM

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

1. Make sure that the PrivateArk Server Service is not running.
2. Run the `CAVaultManager` command line tool of CyberArk with following parameters:
   `CAVaultManager GenerateKeyOnHSM /ServerKey`

The above command will generate a new key for the PrivateArk Server Service and store it in the HSM PKCS#11R2 slot previously initialized, and will return the key generation keyword. For example: HSM#5. Each time a key generation is done, the keyword allocated is one number higher than the current server key generation specified in DBParm.ini. The HSM can store up to 255 key generations, after which key generation numbering will begin again at one. In order to create additional key generations successfully, users have to manually delete the first generation of the server key, otherwise an error will be returned. If the ServerKey parameter in the CAVaultManager command specifies a path instead of an HSM keyword, the first key generation will be created, i.e., HSM#1.

3. Next the Vault data and metadata have to be re-encrypted with the newly generated keys on the HSM. With the use of the command line tool `ChangeServerKeys` run the following command:
   `ChangeServerKeys <PathToKeys> <PathToEmergencyFile> HSMKeyword`

   For example, the following command will re-encrypt the Vault data and metadata with the encryption keys in `K:\PrivateArk\Keys`, and the `HSM#1` key will be used as the server key.

   ```
   ChangeServerKeys K:\PrivateArk\Keys
       K:\PrivateArk\Keys\VaultEmergency.pass HSM#1
   ```

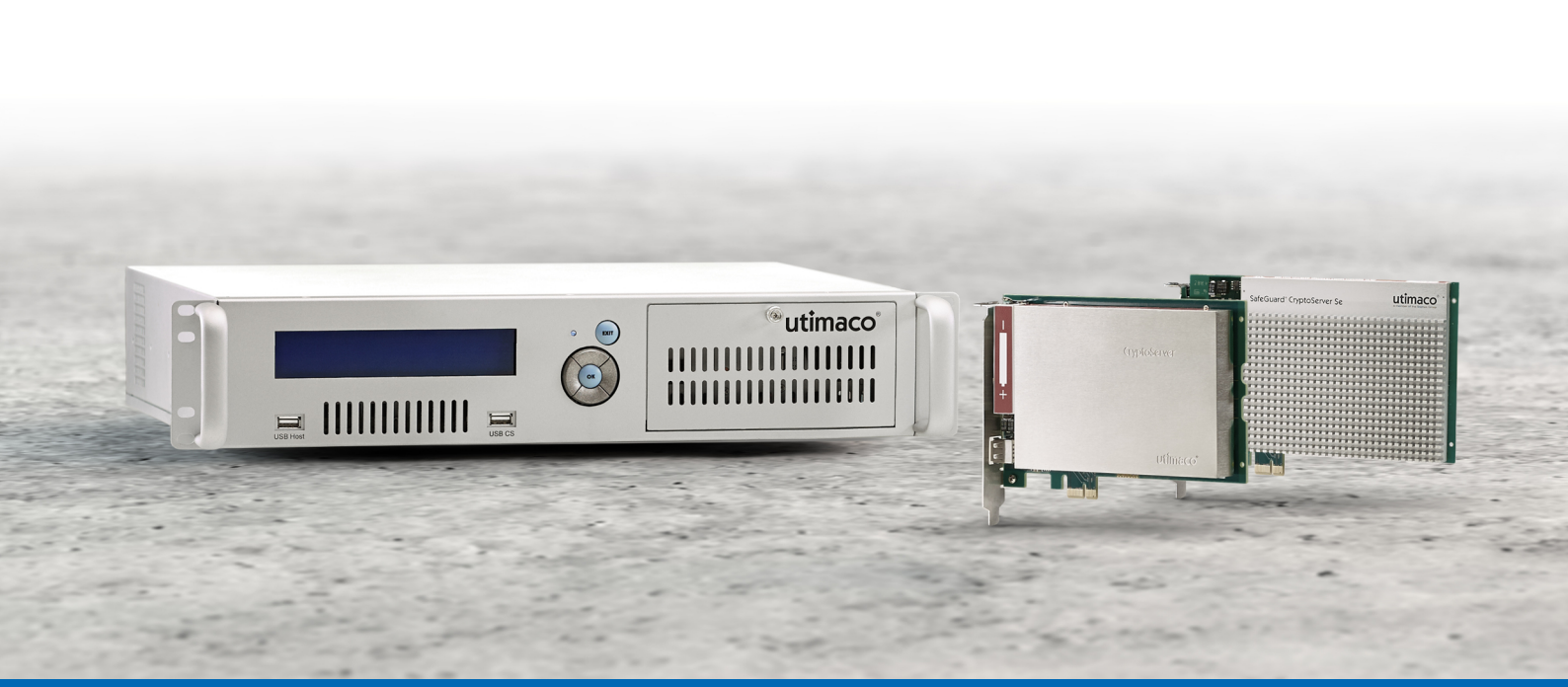
4. After that open the DBParm.ini and edit the `ServerKey` according to the value output of the previous command. For example:
   `ServerKey=HSM#1`
5. Finally, start the PrivateArk Server Service and verify that you can log onto the Vault.

With the above described procedure you have successfully generated the PrivateArk Server Service Key in the PKCS#11 slot on the HSM and can proceed with the installation of of the admin client as described in CyberArk's installation guide.

7 Further Information

This document forms a part of the information and support which is provided by the 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: http://hsm.utimaco.com



Contact

Utimaco IS GmbH
Germanusstraße 4
D - 52080 Aachen
Germany

phone +49 241 1696 - 200
fax +49 241 1696 - 199

web https://hsm.utimaco.com
email support-cs@utimaco.com