gemalto
security to be free

HSMoD Service

CYBERARK DIGITAL VAULT INTEGRATION GUIDE

Document Information

Product Version	1.7
Document Part Number	007-013897-001
Release Date	21 November 2018

Revision History

Revision	Date	Reason
Rev. A	17 August 2017	For initial release 1.1.0
Rev. B	19 September 2017	For release 1.1.1
Rev. C	14 November 2017	For release 1.2
Rev. D	05 February 2018	For release 1.3
Rev. E	02 March 2018	For HSM on Demand release 1.3
Rev. F	05 April 2018	For release 1.4
Rev. G	07 May 2018	For HSM on Demand release 1.4
Rev. H	10 June 2018	For release 1.5
	12 September 2018	For release 1.6
	21 November 2018	For release 1.7

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service, or loss of privacy.

SafeNet Data Protection on Demand1.7

CYBERARK DIGITAL VAULT INTEGRATION GUIDE

Contents

Overview 5
Third Party Application Details 5
Supported Platforms 5

Preparing for the Integration 7
Setup CyberArk Digital Vault 7
Provision HSMoD Service 7
Adding a Service 7
Adding a Service Client 8
Initializing the HSM 9
Constraints on HSMoD Services 10

Integrating CyberArk Digital Vault with an HSM on Demand Service 11
Generating a CyberArk Vault Key on an HSM on Demand Service 11
Configuring the CyberArk Vault 11
Generating a Server Key on an HSM on Demand Service 11

Overview

This document will guide security administrators through the steps for integrating CyberArk Digital Vault with an HSM on Demand Service. It demonstrates securing a CyberArk Digital Vault's top-level encryption key within an HSM.

The CyberArk Privileged Account Security Solution provides 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, and the data stored within the database, CyberArk has designed a multi-layered encryption hierarchy that uses FIPS 140-2 compliant encryption. Each individual file and safe within the Digital Vault database is encrypted with its own unique encryption key. The Digital Vault Server uses key-hierarchy for protecting each object in the Vault. Based on this unique and highly secure approach, CyberArk has the top-level encryption key (server key) which is required to start the Digital Vault.

This document describes how to store server key (encryption key) on SafeNet HSMs.

The benefits of securing the server key with SafeNet HSM include:

- Secure generation, storage, management, and protection of the encryption keys on a FIPS 140-2 level 3 validated hardware*.
- Full life-cycle management of keys.
- Performance improvements resulting from off-loading cryptographic operations from application servers to the HSM on Demand Service.

*Validation in progress

This document contains the following sections:

- "Preparing for the Integration" on page 7
- "Integrating CyberArk Digital Vault with an HSM on Demand Service" on page 11

This overview contains the following topics:

- "Third Party Application Details" below
- "Supported Platforms" below

Third Party Application Details

This integration guide uses the following third party applications:

- CyberArk Digital Vault server
- PrivateArk Client

Supported Platforms

Below is the list of the platforms tested with the following HSMs:

SafeNet Data Protection on Demand (DPoD): is a cloud-based platform that provides on-demand HSM and Key Management services through a simple graphical user interface. With DPoD, security is simple, cost effective and easy to manage because there is no hardware to buy, deploy and maintain. As an Application Owner, you click and deploy services, generate usage reports and maintain only the services that you need.

CyberArk Vault Server	PrivateArk Client	Operating System
10.3	10.3	Windows Server 2012R2

Preparing for the Integration

Before you proceed with the integration, ensure that you have completed the following:

> "Setup CyberArk Digital Vault " below
> "Provision HSMoD Service" below

Setup CyberArk Digital Vault

CyberArk Vault and PrivateArk Client must be installed on the target machine to complete the integration process. Refer to the *CyberArk Application Guide* and *CyberArk Administrator's Operations Manual* for more information on installation procedures.

Provision HSMoD Service

The HSM on Demand Service provides your client machine with access to an HSM application partition for storing cryptographic objects used by your applications. Application partitions can be assigned to a single client, or multiple clients can be assigned to, and share, a single application partition.

You must provision your HSM on Demand service by adding the service, downloading the service client package and initializing the HSM. Provisioning your HSM on Demand service entails:

> "Adding a Service" below
> "Adding a Service Client" on the next page
> "Initializing the HSM" on page 9

Adding a Service

1. Under the **Services** tab, select the **Add New Service** page. Click **Deploy** on the service tile for the service you wish to add.

   NOTE Click **Deploy** on the HSM on Demand Service tile for your integration.

2. Review the "Terms of Services DPoD." Enable the **I have read and accept the Terms of Service above** check box and then click **Next**.
3. On the **Add <service_type> Service** page, enter a name for the Service in the **Service Name** field. You can optionally allow non-FIPS approved algorithms by selecting the **Allow non-FIPS approved algorithms** check box. Click **Next**.

   CAUTION! You cannot alter the FIPS setting after creating the service. You must decide if the service should allow or disallow non-FIPS approved algorithms before clicking **Finish** in the next step.

4. Review the configuration summary page. If acceptable, click **Finish**. If you would like to make changes to the configuration, click **Go Back**.

When completed, the new service is listed under **My Services** and a **Create Service Client?** window displays.

5. Click **Create Service Client**.

Adding a Service Client

1. In the **Create Service Client** window enter a name for the service client in the **Service Client Name** field.

> **NOTE** If the **Create Service Client** window is not available, navigate to the **Services** tab and click the name of the Service you would like to generate a client for in the **My Services** table. On the Service Details page, click **New Service Client**.

2. Select **Create Service Client**.

   A new HSM service client package is created and provided for downloading on your client system.

> **NOTE** The HSM service client package is a zip file that contains system information needed to connect your client system to an existing HSM on Demand service. The HSM service client package should download immediately on creation. If it does not, or you lose access to your HSM service client package it can be accessed or reacquired through the **My Services** table.

3. Transfer the service client package to your client system. You can use SCP, PSCP, WinSCP, FTPS, or any other secure file transfer tool.
4. Unzip the service client package.

   For Linux, enter:

   ```
   unzip <service_client_package>.zip
   ```

   For Windows, using the Windows GUI or an unzip tool unzip the file:

   ```
   <service_client_package>.zip
   ```

> **NOTE** For more information about the service client package contents see .

5. Extract the cvclient-min file.

> **NOTE** Extract the cvclient-min file in the directory where you extracted the <service_client_package>.zip. **Do not** extract to a new cvclient-min directory.

   For Linux, untar the cvclient-min.tar

   ```
   tar xvf cvclient-min.tar
   ```

   For Windows, unzip the cvclient-min.zip.

6. Set the environment variable.

   For Linux, execute:

```
source ./setenv
```

For Windows, right click setenv.cmd and select **Run as Administrator**.

> **NOTE** If you encounter the error dll load failed with GetLastError() 126 move the contents of the cvclient_min folder up one directory and execute setenv.

7. Start LunaCM.

   For Linux, execute the following from the directory where you extracted the cvclient-min.tar file.

   ```
   ./bin/64/lunacm
   ```

   For Windows, execute the following from the directory where you unzipped the cvclient-min.zip file.

   ```
   lunacm
   ```

Initializing the HSM

1. Set the active slot to the service partition.

   ```
   lunacm:>slot set -slot <slot_number>
   ```

   > **NOTE** Execute slot list in LunaCM to identify the slot number associated with your service.

2. Initialize the application partition. During this process you will create the partition's Security Officer (SO), set the SO password, and specify the cloning domain.

   ```
   lunacm:> partition init -label <service_label>
   ```

3. Optional: If you wish to transfer key material to or from a PED-authenticated Luna partition, you initialize the SafeNet Data Protection On Demand partition using the red PED domain key.

   a. For DPoD deployments, contact customer support to obtain the necessary PED drivers so that your HSM client can communicate with the PED.

   b. Attach the PED locally to the client computer, insert the red cloning domain PED key, and initialize the partition, including the option to set the cloning domain from the red PED key. Execute:

      ```
      lunacm:> partition init -label <cryptovisor_partition_label> -importpeddomain
      ```

4. Log in as the partition's Security Officer:

   ```
   lunacm:>role login -name Partition SO
   ```

5. Initialize the Crypto Officer role:

   ```
   lunacm:>role init -name Crypto Officer
   ```

6. Log out of the partition Security Officer role and log in as the Crypto Officer.

   ```
   lunacm:>role logout
   lunacm:>role login -name Crypto Officer
   ```

7. You must change the Crypto Officer password immediately on the initial log in. Failure to due so will result in a password error on subsequent logins.

   ```
   lunacm:>role changepw -name Crypto Officer
   ```

8. Initialize the Crypto User role:

```
lunacm:>role init -name Crypto User
```

9. Log out of the partition Crypto Officer role and log in as the Crypto User.

```
lunacm:>role logout
lunacm:>role login -name Crypto User
```

10. You must change the Crypto User password immediately on the initial log in. Failure to do so will result in a password error on subsequent logins.

```
lunacm:>role changepw -name Crypto User
```

This completes initializing the HSM on Demand Service. The Crypto Officer and Crypto User roles can now be used to integrate applications with the HSMoD service to perform cryptographic operations

Constraints on HSMoD Services

Please take the following limitations into consideration when integrating your application software with an HSM on Demand Service.

HSM on Demand Service in FIPS mode

HSMoD services operate in a FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, ensure you enable the **Allow non-FIPS approved algorithms** check box when configuring your HSM on Demand service. The FIPS mode is enabled by default.

Refer to the *Mechanism List* in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.

Verify HSM on Demand <slot> value

LunaCM commands work on the current slot. If there is only one slot, then it is always the current slot. If you are completing an integration using HSMoD services, you need to verify which slot on the HSMoD service you send commands to. If there is more than one slot, then use the **slot set** command to direct a command to a specified slot. You can use **slot list** to determine which slot numbers are in use by which HSMoD service.

Integrating CyberArk Digital Vault with an HSM on Demand Service

This integration contains the following topics:

> "Generating a CyberArk Vault Key on an HSM on Demand Service" below

Generating a CyberArk Vault Key on an HSM on Demand Service

After installing the Vault, the server key can be generated on the HSM on Demand service, where it will be stored as a non-exportable key.

Configuring the CyberArk Vault

To use an HSM on Demand service with CyberArk Vault you must configure the server parameter file to use the HSMoD service.

To configure the CyberArk Vault

1. Configure the PKCS#11 provider DLL. Open the **dbparam.ini** file in a text editor and configure the PKCS11ProviderPath parameter to point to the PKCS#11 provider DLL. In the [Main] section add:

   PKCS11ProviderPath=<path_to_PKCS#11_provider_.dll>

   Example:

   PKCS11ProviderPath="C:\Program Files\SafeNet\LunaClient\cryptoki.dll"
2. Navigate to C:\Program Files(x86)\PrivateArk\Server. Execute the CAVaultManager command and enter the service password that will be used to access the server key:

   CAVaultManager.exe SecureSecretFiles /SecretType HSM /Secret <service_password>
3. Open **dbparam.ini** and verify that the HSMPinCode parameter was added with the encrypted value of the PIN code.
4. Restart the CyberArk Server to apply the new firewall rules.
5. Shutdown the CyberArk server.

Generating a Server Key on an HSM on Demand Service

You can generate the server encryption key for CyberArk Vault using the HSMoD service.

To generate a server key on an HSMoD service

1. Verify the CyberArk Digital Vault Server is offline.
2. Navigate to C:\Program Files(x86)\PrivateArk\Server. Run the CAVaultManager command and generate a server key on the HSMoD service.

   CAVaultManager.exe GenerateKeyOnHSM /ServerKey

> **NOTE** This command generates a new key for the Vault server and stores the Vault server key on the HSMoD service. Additionally, the Vault server key generation command also returns the key generation keyword to the user. We recommend saving the key generation keyword in a secure place on your system, as you will require it for subsequent steps in the integration.

Copy the Key generation keyword. You will require this value for a command later.

3. Open the **dbparam.ini** file and verify that the RecoveryPrvKey section points to the correct private recovery key (recprv.key)
4. Navigate to **C:\Program Files(x86)\PrivateArk\Server** and execute the **ChangeServerKeys** command to change the encryption keys that will be used for the Vault server.

> **NOTE** This command re-encrypts the Vault data and metadata with the encryption keys.

ChangeServerKeys <path_to_server_key> <path_to_emergency_file> <HSM_keyword>

For Example:

ChangeServerKeys C:\Keys C:\Keys\VaultEmergency.pass HSM#1

5. Open the **dbparam.ini** file and in the ServerKey parameter section specify the key generation keyword that was generated in the output in the CAVault Manager command.

   ServerKey=HSM#1

6. Start the Vault server and log in.

   This completes the integration of CyberArk Vault with SafeNet HSM.