

Integrating CyberArk Vault with Atos-Bull HSM Protezione



Introduction

One of the unique capabilities of CyberArk's patented Digital Vault technology is the ability to manage encryption keys transparently. Each account or file in the Vault is encrypted with its own unique encryption key. The Digital Vault Server uses sophisticated key-hierarchy for protecting each object in the Vault. Based on this unique and highly secure approach, CyberArk protects the top-level encryption key in a Hardware Security Module (HSM) device as non-exportable. Customers who would like to leverage an HSM to further maximize the security of cryptographic keys used by the CyberArk Solution can benefit from a highly secure solution based on this out of box integration. The Digital Vault communicates with the HSM devices using PKCS#11 protocol.

Encryption keys can be stored on the HSM device in either of the following ways:

- Existing keys can be loaded onto the HSM device
- New keys can be generated directly on the HSM device

This document describes how to store encryption keys on Atos-Bull Proteccio HSM device, and how to integrate the Proteccio HSM with the CyberArk Digital Vault.

Integration environment

The integration test was performed in below environment:

OS: Windows Server 2012 R2 64 bits and Windows Server 2008 R2 64 bits

Vault: V9.5

Atos-Bull HSM : Proteccio

Note: Performance impact on the CyberArk Digital Vault was not measured during this test.



Integration steps

Installing Proteccio HSM PKCS#11 library

- 1- Run the setup.exe under Windows/Java6or7 directory in the Proteccio CD drivers and follow installation steps.
- 2- Unzip the Proteccio 64 bits dll libraries under %windir%\System32\
- 3- Configure the proteccio.ini file under %windir%\proteccio\ to reflect your configuration

```
[PROTECCIO]
IPAddr=<HSM IP Address>
SSL=<0 no SSL, 1 use SSL>
SrvCert=<HSM Server Certificate Path, ignored if no SSL>

[CLIENT]
Mode=0
LoggingLevel=<from 0 lowest debug level to 7>
LogFile=<Path to log file>
ClntKey=<Path to Vault machine certificate private key file, ignored if no SSL>
ClntCert=< Path to Vault machine certificate file, ignored if no SSL>
```

Initial Vault Configurations

- 1- Configure the Firewall in order to allow communication to the HSM device. In DBParm.ini, configure the AllowNonStandard FWAddresses parameter to open the Firewall and allow access to the HSM device, as shown in the following example (please replace ##### for the particular port or port range that needs to be opened to allow the communication):

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

- 2- Specify the Proteccio PKCS#11 provider 64 bits DLL in the PKCS11ProviderPath parameter in DBParm.ini, as shown in the following example:

```
[HSM]
PKCS11ProviderPath="C:\Windows\System32\nethsm.dll"
HSMSlotIndex=<slot number where Vault Keys will be stored>
```

- 3- Save DBParm.ini and close it.
- 4- From a command line, run the following command, specifying the PIN code that will be used to access the HSM:

```
CAVaultManager SecureSecretFiles /SecretType HSM /Secret <HSM PIN CODE>
```



Open DBParm.ini and make sure that the HSMPinCode parameter was added with the encrypted value of the PIN code.

- 5- Restart the PrivateArk Server to apply the new Firewall rules.
- 6- Shutdown the PrivateArk Server.

Loading the Server Key into the HSM

The following process installs and stores the Server key on the HSM device. Once this process is complete, the server key is stored as non exportable key on the HSM and will be used by the Vault.

- 1- Make sure that the Vault Server is not running.
- 2- From a command line, run the following command:

```
CAVaultManager.exe LoadServerKeyToHSM
```

- 3- Make sure that the result confirms that the Server key has been loaded to the HSM.
- 4- In DBParm.ini, change the value of the ServerKey parameter as follows:

```
ServerKey=HSM
```

- 5- Start the Vault server and make sure you can log on.

The Server key has been successfully moved to the HSM and will be used for all relevant CyberArk Vault operations.

Generating the Server Key in the HSM

- 1- Make sure that the Vault Server is not running.
- 2- Run the CAVaultManager command to generate the server key on the HSM:

```
CAVaultManager GenerateKeyOnHSM /ServerKey
```

The above command will generate a new key for the Vault server and store it in the HSM device, and will return the key generation keyword. For example: HSM#5

Each time a key generation is created, 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- Re-encrypt the Vault data and metadata with the newly generated keys on the HSM.

Run the ChangeServerKeys command to change the encryption keys that will be used for the Vault server.



ChangeServerKeys PathToMasterKeys 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- Open DBParm.ini and in the ServerKey parameter specify the value of the key generation version that was generated and specified in the output of the CAVaultManager command above, as shown in the following example.
- 5- Start the Vault server and make sure you can log on.

