# Black•Vault HSM Microsoft CA Integration Guide

© Engage Black 9565 Soquel Drive Aptos, CA 95003 Phone +1 831.688.1021 1 877.ENGAGE4 (364.2434) sales@engageblack.com

# **Disclaimer and Warranty**

Engage Black is a business unit of Engage Communication.

©2016 Engage Communication, Inc. All rights reserved. This document may not, in part or in entirety, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without first obtaining the express written consent of Engage Communication. Restricted rights legend: Use, duplication, or disclosure by the U.S. government is subject to restrictions set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 52.227-7013 and in similar clauses in the FAR and NASA FAR Supplement.

Information in this document is subject to change without notice and does not represent a commitment on the part of Engage Communication, Inc. Product specifications are subject to change without notice. Engage Communication assumes no responsibility for any inaccuracies in this document or for any obligation to update the information in this document.

Engage Communication, Inc. and the Engage Communication logo are registered trademarks of Engage Communication, Inc. All other trademarks and service marks in this document are the property of Engage Communication, Inc., or their respective owners.

Engage Communications, Inc. 9565 Soquel Drive Aptos, CA 95003

Phone +1(831) 688-1021

http://www.engageblack.com/

http://www.engageinc.com/

Sales +1 (831) 688-1021 sales@engageblack.com

Global Technical Support +1 (831) 688-1021 (extension 3) <a href="mailto:support@engageblack.com">support@engageblack.com</a>

## **Table of Contents**

1. Introd	uction
2. Proced	lure5
2.1. Integra	tion with MSCA
2.1.1. In:	stalling Active Directory Certificate Services5
2.1.2. Co	onfiguring the Active Directory Certificate Authority10
2.2. Setting	Up Internet Information Services (IIS) For Certification Authority Web
Enrollment (o	ptional)
2.3. Using I	MSCA
2.3.1. Im	port CSR
2.3.1.1.	Via web
2.3.1.2.	Via certsrv
2.3.2. Iss	sue certificate
2.3.2.1.	Via certsrv
2.3.3. Ex	port cert
2.3.3.1.	Via web
2.3.3.2.	Via certsrv
2.3.4. Re	evoke cert
2.3.4.1.	Via certsrv

# **1.** Introduction

A primary security control in a Public Key Infrastructure (PKI) is how the private keys are stored and managed, especially when it concerns Certification Authorities (CAs). A strong key protection strategy is critical to maintaining and ensuring security. The BlackVault HSM enhances the security of CAs and PKIs. It does this by providing an easy to use, hardware based secure storage system of the private keys, as well as providing a dedicated cryptographic processor to perform the desired cryptographic operations.

Microsoft uses its cryptographic API interfaces to talk to the BlackVault HSM. When Windows is interfacing with a BlackVault HSM, the HSM functions as a Cryptographic Services Provider (CSP). To use the BlackVault HSM as a CSP with a Microsoft CA, the BlackVault HSM libraries must be installed and the BlackVault HSM must be correctly set up and in the operational state.

It is highly recommended that a strong protection strategy is taken when using the BlackVault HSM. This includes ensuring that the BlackVault HSM resides in a secure place, storing the smart cards associated with the operators of the BlackVault correctly, and properly backing up the BlackVault HSM databases (user and smart card).

For a complete installation and use guide for the Microsoft CA, please consult Microsoft documentation. This guide should be used more as an overview on how to integrate the BlackVault HSM with the Microsoft CA.

The benefits of using a BlackVault HSM with Microsoft CA include:

- Secure storage of the private key
- Signing code within a cryptographically secure environment
- FIPS 140-2 level 3 validated hardware

# 2. Procedure

To proceed the following is needed:

- BlackVault HSM
- BlackVault smart card set
- BlackVault HSM setup CD
- A client computer that has a supported Operating System installed.

Additionally, the BlackVault HSM must be Initialized and Configured properly (see the BlackVault HSM User Guide for more details).

To setup Microsoft CA with the BlackVault HSM:

• Install the BlackVault HSM Libraries onto the Client Machine by running the application bysetup.exe (included in the setup folder)

The following assumes you already initialized the BlackVault HSM and are installing this software on a machine that does not already have a Microsoft CA setup.

# **2.1.** Integration with MSCA

## 2.1.1. Installing Active Directory Certificate Services

- 1. Copy the already configured pkcs.dat to C:\Windows\System32\. Alternatively, you can set the BV\_PKCS\_PATH system environment variable to specify the path to the pkcs.dat file.
- 2. Log into BlackVault HSM as User

- 3. Add Microsoft Active Directory Certificate services
  - a. Open the Server Manager application
  - b. Under the Manage dropdown menu, select Add Roles and Features

Server Manager	<ul> <li>Dashboard</li> </ul>	• 🕲 I		Manage	Тос
📥 Add Roles and Features Wizard			-		×
Before you begin			DESTI WIN-F	NATION SERVE ROUG9N4VNO	:R N
Before You Begin Installation Type Server Selection Server Roles	This wizard helps you install roles, role services, or features. You de features to install based on the computing needs of your organiza hosting a website. To remove roles, role services, or features: Start the Remove Roles and Features Wizard	etermine which tion, such as sh	roles, ro aring do	le services, o ocuments, or	or r
Features Confirmation Results	Before you continue, verify that the following tasks have been com • The Administrator account has a strong password • Network settings, such as static IP addresses, are configured • The most current security updates from Windows Update are ins If you must verify that any of the preceding prerequisites have been complete the steps, and then run the wizard again.	npleted: talled en completed, c	lose the	wizard,	
	To continue, click Next.				
	< Previous Next >	Ins	tall	Cancel	

- c. A prompt for installation type will appear. Select **Role-based or feature-based installation** then press Next to continue.
- d. The next screen prompts to select **destination server**. Press Next to continue.
- e. Select all role services that are needed. The only role required for this configuration is **Active Directory Certificate Services.**

📥 Add Roles and Features Wizard		- 🗆 X
Add Roles and Features Wizard  Select server roles  Before You Begin Installation Type Server Selection  Server Roles  Features AD CS Role Services Confirmation Results	Select one or more roles to install on the selected server. Roles	– C X DESTINATION SERVER WIN-ROUG9N4VNON Description Active Directory Certificate Services (AD CS) is used to create credification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
	Remote Access  Remote Desktop Services  Volume Activation Services	
	Web Server (IIS) Windows Deployment Services Windows Server Update Services V	
	< Previous Next	> Install Cancel



© Engage Black

- f. The next screen is to **Select Features**. Press Next to continue.
- g. The next screen is the description of Active Directory Certificate Services. Press Next to continue.
- h. On the Select role services page, select the role services required for this installation (at least Certification Authority), and press Next to continue.

📥 Add Roles and Features Wizard		- 🗆 ×
Select role service	5	DESTINATION SERVER WIN-R0UG9N4VNON
Before You Begin	Select the role services to install for Active Directory Certificate	Services
Installation Type	Role services	Description
Server Selection Server Roles Features AD CS Role Services Confirmation Results	Certification Authority     Certificate Enrollment Policy Web Service     Certificate Enrollment Web Service     Certification Authority Web Enrollment     Detwork Device Enrollment Service     Online Responder	Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.
	< Previous Next	> Install Cancel

Note: In the last section of this guide, we supply examples of basic MSCA function via web. If you wish to perform functions via web you must also select **Certification Authority Web Enrollment.** 

i. On the Confirmation page press Install.

📥 Add Roles and Features Wizar	d	-		×
Confirm installat	ion selections	DESTINA WIN-RO	ATION SERV DUG9N4VN	/ER ON
Before You Begin Installation Type	To install the following roles, role services, or features on selected server, click Install the destination server automatically if required	stall.		
Server Selection Server Roles	Optional features (such as administration tools) might be displayed on this page been selected automatically. If you do not want to install these optional features their check boxes.	because ti , click Prev	hey have ious to cl	ear
AD CS Role Services Confirmation Results	Active Directory Certificate Services Certification Authority Remote Server Administration Tools Role Administration Tools Active Directory Certificate Services Tools Certification Authority Management Tools			
	Export configuration settings Specify an alternate source path			
	< Previous Next > In	stall	Cance	el -

Note: This page will show more information if you chose to install Certification Authority Web Enrollment as well.

j. After the wizard has finished installing, on the Results page, press Close

## 2.1.2. Configuring the Active Directory Certificate Authority

1. Select the notification flag in the right-hand corner of the Server Manager application.



4. On the **Role Services** page, select the roles you wish to configure (choosing at least **Certificate Authority**) and press Next.

AD CS Configuration		- 🗆 ×
Role Services		DESTINATION SERVER WIN-ROUG9N4VNON
Credentials Role Services	Select Role Services to configure	
Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Certification Authority Certification Authority Web Enrollment Online Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service More about AD CS Server Roles	
	< Previous Next >	Configure Cancel

Note: If you decided to install Certification Authority Web Enrollment, select that as well.

#### 5. On the Setup Type page, select standalone CA and press Next



6. On the CA Type page, choose CA type (root ca for this example) and press Next



7. On the Private Key page, select "Create a new private key" and press Next



- 8. Next is the Cryptography for CA page
  - i. In the **Select a cryptographic provider** drop down menu, select one of the Engage Black-Vault Cryptography Providers, this includes:
    - ECDSA\_P256#Engage BlackVault Cryptography Provider
    - ECDSA\_P384#Engage BlackVault Cryptography Provider
    - RSA#Engage BlackVault Cryptography Provider
    - RSA\_SIGN#Engage BlackVault Cryptography Provider

Note: In this example we are using RSA#Engage BlackVault Cryptography Provider

ii. Specify the key length and hash algorithm of your choice

📥 AD CS Configuration		- 🗆 ×	ζ
Cryptography for	CA	DESTINATION SERVER WIN-R0UG9N4VNON	
Credentials	Specify the cryptographic options		
Role Services			
Setup Type	Select a cryptographic provider:	Key length:	
СА Туре	RSA#Engage BlackVault Cryptography Provider *	2048 *	
Private Key	Select the hash algorithm for signing certificates issued by this CA:		
Cryptography	SHA256 ^		
CA Name	SHA384		
Validity Period	SHA512		
Certificate Database	SHA1		
Confirmation	MD5		
	$\hfill \square$ Allow administrator interaction when the private key is accessed	by the CA.	
	More about Cryptography		
	< Previous Next >	Configure Cancel	

9. On the CA name page, enter in the Common name, and the Distinguished name in the appropriate fields then press Next.

AD CS Configuration		-		×
CA Name		DESTINAT WIN-ROU	ion ser Jg9N4VN	VER
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Specify the name of the CA Type a common name to identify this certification authority (CA). This certificates issued by the CA. Distinguished name suffix values are auto be modified. Common name for this CA: EXAMPLE Distinguished name suffix: Preview of distinguished name: CN=EXAMPLE More about CA Name	s name is added t tomatically gener	to all ated but	can
	< Previous Next >	Configure	Cance	ł

10. On the Validity Perion page, select the how long you want the CA to remain valid, then press Next.

AD CS Configuration	- 🗆 X	
Validity Period	DESTINATION SERVER WIN-R0UG9N4VNON	
Credentials Role Services	Specify the validity period	
Setup Type CA Type	Select the validity period for the certificate generated for this certification authority (CA):           5         Years         Years	
Private Key Cryptography CA Name	CA expiration Date: 1/6/2026 4:45:00 PM The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.	
Validity Period Certificate Database		
Confirmation Progress		
	More about Validity Period	
	< Previous Next > Configure Cancel	

11. On the CA Database name, if you want the database and log locations in a different place than default, choose so now, then press Next.

12. On the confirmation screen, review the configuration, then press Configure

AD CS Configuration			-		×
Confirmation			DESTINAT WIN-ROU	ION SER	VER ON
Credentials Role Services Setup Type	To configure the following roles, <ul> <li>Active Directory Certificat</li> </ul>	role services, or features, click Configure. e Services			
CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Certification Authomy CA Type: Cryptographic provider: Hash Algorithm: Key Length: Allow Administrator Interaction: Certificate Validity Period: Distinguished Name: Certificate Database Location: Certificate Database Log Location:	Standalone Root RSA#Engage BlackVault Cryptography Pro SHA256 2048 Disabled 1/6/2026 4:45:00 PM CN=EXAMPLE C:\Windows\system32\CertLog C:\Windows\system32\CertLog	vider		
		< Previous Next > Cor	figure	Cance	4

- 13. The configuration will now begin, once the results screen shows up, press Close to complete the process.
- **14.** To verify the CA configuration, in the **Server Manager tools** dropdown menu, select **Certification Authority.**

🙀 certsrv - [Certification Authority	(Local)]		_	$\times$
File Action View Help				
🔃 🔿 📄 🛃				
Certification Authority (Local)	Name	Description Certification Authority		

## **2.2.** Setting Up Internet Information Services (IIS) For Certification Authority Web Enrollment (optional)

This section will describe how to set up Internet Information Services for Certification Authority Web Enrollment, you will need a proper SSL certificate for this.

1. From the Server Manager Tools dropdown menu, select Internet Information Services.

Internet Information Services (IIS)	Manager	-		$\times$
← → ♥ Start Page		<b>1</b>	× 🏠	• 🕥
File View Help				
Connections	Morosoft Application Server Manager Recent connections WIN-ROUG9N4VNON WIN-ROUG9NAVNON WIN-ROUG9NAVNON WIN-ROUG9NAVNON	Online reso IIS News an IIS Downloa IIS Forums TechNet MSDN ASP.NET N Enat	purces id Inform ads ews ple IIS N ws.	ews
Ready				:

- 2. In the **Connections** list (on the left), select your server
  - a) Locate the Server Certificates feature. Right click on the icon and select Open Feature

Internet Information Services (IIS) I	Manager				-		×
← → ♥in-Roug9N4V	NON 🕨				<b>5</b>	🛛 🟠	• 🕥
File View Help							
Connections	Server Certifica Use this feature to request and m the Web server can use with web Filter:	tes anage certificates that sites configured for SSL. Go C Show All Issued To EXAMPLE	Ret	tions Import Create Ce Complete Create De Create Se Enable At Renewed Help	ertificat e Certifi pmain h If-Sign utomat Certifi	e Reque icate Rei Certifica ed Certifi ic Rebin cate	st iuest icate d of
< > > Ready	Content view	**					• <u>1</u> .:

b) Under the Actions table on the right, select Import...

115 Internet Information Services (IIS	) Manager	- 🗆 X
← → ♥ WIN-ROUG9N4	IVNON 🕨	😰 📧 🏠 i 🔞 🗸
File View Help		
Connections	Import Certificate 2 X	Actions
🔍 - 🔒 🖄 😥		Import
Start Page	Certificate file (.pfx):	Create Certificate Request
Application Pools		Create Domain Certificate
> "M Siles	Password:	Create Self-Signed Certificate
		Enable Automatic Rebind of Renewed Certificate
	Select Certificate Store:	🕡 Help
	Personal V	
	Allow this certificate to be exported	
	OK Cancel	_
	< >>	
< >	Features View 🚰 Content View	
Ready		¶.:

- c) Import your SSL certificate
- 3. Double click on your server name in the **Connections** list on the left
- 4. Double click on **Sites** in the dropdown menu
- 5. Click on **Default Web Site**

Internet Information Services (IIS)	Manager	– 🗆 X
← → WIN-R0UG9N4V	NON 🕨 Sites 🕨 Default Web Site 🕨	😰 🛛 🟠 🔞 🗸
File View Help		
Connections	Default Web Site Home	Actions
😪 - 🔒 🖄 😸		🔉 Explore
Start Page	Filter: 👻 🐨 🖓 Go 🗟 🖓 🖓 🚽	Edit Permissions
Application Pools		Edit Site
✓ 🙆 Sites	ی 🕵 🧟	Bindings
> 🥹 Default Web Site	ASP Authentic Compression	View Applications
		View Virtual Directories
		Manage Website
	Default Directory Error Pages	🗢 Restart
	Document Browsing	Start
		Stop
	Failed Handler HTTP	Browse Website
	Request Tra Mappings Redirect	Advanced Settings
		Configure
		Failed Request Tracing
< >>	🛅 Features View ि Content View	Limits 🗸
Ready		• <b>1</b> .:

- a) Select Bindings in the Actions panel on the right
- b) Click Add...
- c) Change the type to https
- d) Select your SSL certificate

Add Site Binding	9					?	×
Туре:		IP address:		Port:			
https	$\sim$	All Unassigned		~ 443			
Host name:				_			
Require Ser	ver Nam	e Indication					
Disable HT	TP/2						
Disable OC	SP Stapli	ng					
SSL certificate:	1						
SSLcert			~	Select	V	iew	
				OK	(	Cancel	

- 6. Double click on the **Default Web Site** item in the **Connections** list
- 7. Click on CertSrv and then click on Browse \*:443 (https) in the Actions panel
- © Engage Black Document Number: BVH-MSCAIG-7010

Internet Information Services (IIS) I	Manager					_		×	
← → WIN-R0UG9N4VI	NON 🕨 Sites 🕨	Default W	eb Site 🔸			<b>5</b>	⊠ 🏠	• 1	
File View Help									
Connections	Dof		o Sito Homo	A	ctions				
🔍 - 🔚 🖄 🔛				j,	Explore			^	
Start Page	Start Page Filter: - 🐨 Go - 🕁 Show All _		-	Edit Pern	issions	5	_		
Application Pools	Ø	Ξ₽	404	^	Edit Site				
V 🙆 Sites	Default Directory		Error Pages		Bindings				
Default Web Site     Site     Site     Site	Document browsing			View Applications			_		
> 🔐 CertSrv	8				View Virt	ual Dire	ectories		
	Failed Request Tra	Handler Mannings	HTTP Redirect	м	Manage Website				
	HTTP Logging	P	2	Restart					
			<b>1</b>		<ul><li>Start</li><li>Stop</li></ul>				
		Logging	MIME Types						
	Respon				Browse	Nebsit	e		
			6		Browse *	80 (htt 443 (ht	p) tos)		
	Modules	Output	Request		Advance	d Sattin			
		Caching	riitering	×	Configur	a secon	.ga		
< >	Features View	v ह Conte	nt View		Failed Re	quest T	racing	~	
Ready								€ .:	

8. You should now have access to the Microsoft Active Directory Services web interface

Microsoft Active Directory Certificate Services EXAMPLE	Home
Welcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificat can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending the type of certificate you request, perform other security tasks.	ite, you g upon

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see <u>Active Directory Certificate Services</u> <u>Documentation</u>.

Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>

# 2.3. Using MSCA

These are brief snippets of some of the basic functions the MSCA can do, for full details, please consult the Microsoft documentation.

## 2.3.1. Import CSR

#### 2.3.1.1. Via web

- 1. Open a Web browser.
- 2. You can open **https://servername/certsrv**, where *servername* is the name of the server hosting the CA Web enrollment pages or open the browser as we did in step 7 of the previous section.
- 3. Click Request a Certificate then select advanced certificate request
- 4. On Request a Certificate, select Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Note: The first option, create and submit a request to this CA cannot be chosen due to the BlackVault HSM only accepting one transaction at a time.

- 5. On the **Submit a Certificate Request or Renewal Request** page, paste your CSR, select your template, and add any additional attributes.
- 6. Click Submit.
- 7. Do one of the following:
  - a. If the **Certificate Pending** web page appears, see Check on a Pending Certificate Request for the procedure to check on a pending certificate.
  - b. If the Certificate Issued Web page appears, click Install this certificate.

### 2.3.1.2. Via certsrv

- 1. In the Server Manager application, in the Tools dropdown menu, select Certification Authority.
- 2. Select the CA from the pool you wish to request a certificate from.
- 3. In the Action menu, point to All Tasks, and then click Submit New Request.
- 4. This will open a menu; browse to the certificate you want to import and click Open.

## 2.3.2. Issue certificate

#### 2.3.2.1. Via certsrv

- 1. In the Server Manager application, in the Tools dropdown menu, select Certification Authority.
- 2. In the console tree, click **Pending Requests**.
- 3. In the details pane, left click the certificate you want to issue.
- 4. On the Action menu, point to All Tasks, and click Issue

#### 2.3.3. Export cert

#### 2.3.3.1. Via web

- 1. Open a Web browser.
- 2. You can open **https://servername/certsrv**, where *servername* is the name of the server hosting the CA Web enrollment pages or open the browser as we did in step 7 of the previous section.
- 3. Click Download a CA certificate, certificate chain, or CRL.
- 4. Click the encoding method that you want to use for the CRL, **DER** or **Base 64**.
- 5. Do one of the following:
  - Click Download CA certificate.
  - Click Download CA certificate chain.
  - Click **Download latest base CRL**.
  - Click **Download latest delta CRL**.
- 6. When the **File Download** dialog box appears, click **Save**. Select a folder on your computer to store the .crl file, and then click **Save**.
- 7. Open Windows Explorer and locate the .crl file you just saved.
- 8. Right-click the .cer or .crl file and click Install Certificate or Install CRL, and then click Next.
- 9. When the Certificate Import Wizard opens, click **Automatically select the certificate store based on the type of certificate**.

#### 2.3.3.2. Via certsrv

- 1. In the Start Menu, under administrative tools click on **Certification Authority**
- 2. In the console tree under the logical store that contains the certificate to export, click **Certificates**.
- 3. In the details pane, click the certificate that you want to export.
- 4. On the **Action** menu, point to **All Tasks**, and then click **Export**.
- 5. In the Certificate Export Wizard, click **No, do not export the private key**. (This option will appear only if the private key is marked as exportable and you have access to the private key.)
- 6. Provide the following information in the Certificate Export Wizard:
  - Click the file format that you want to use to store the exported certificate: a DERencoded file, a Base64-encoded file, or a PKCS #7 file.
  - If you are exporting the certificate to a PKCS #7 file, you also have the option to include all certificates in the certification path.
- 7. If required, in **Password**, type a password to encrypt the private key you are exporting. In **Confirm password**, type the same password again, and then click **Next**.
- 8. In **File name**, type a file name and path for the PKCS #7 file that will store the exported certificate and private key. Click **Next**, and then click **Finish**.

#### 2.3.4. Revoke cert

#### 2.3.4.1. Via certsrv

- 1. In the Server Manager application, in the Tools dropdown menu, select Certification Authority.
- 2. In the console tree, click **Issued Certificates**.
- 3. In the details pane, left click the certificate you want to revoke.
- 4. On the Action menu, point to All Tasks, and click Revoke Certificate.
- 5. Select the reason for revoking the certificate, adjust the time of the revocation, if necessary, and then click **Yes**.

The following reason codes are available:

- Unspecified
- Key Compromise
- CA Compromise
- Change of Affiliation
- Superseded
- Cease of Operation
- Certificate Hold