Disclaimer and Warranty

Engage Black is a business unit of Engage Communication.

©2017 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.

Engage Communication makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability of fitness for any particular purpose. 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.

All intellectual property is protected by copyright. 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/
Table of Contents

1. Introduction .................................................................................................................. 4
2. Procedure ....................................................................................................................... 5
   2.1. Integration with MSCA .......................................................................................... 5
       2.1.1. Installing Active Directory Certificate Services ........................................... 5
       2.1.2. Configuring the Active Directory Certificate Authority .............................. 10
   2.2. Using MSCA ......................................................................................................... 17
       2.2.1. Import CSR .................................................................................................. 17
           2.2.1.1. Via web .................................................................................................. 17
           2.2.1.2. Via certsrv ............................................................................................ 17
       2.2.2. Issue certificate .............................................................................................. 17
           2.2.2.1. Via certsrv ............................................................................................ 17
       2.2.3. Export cert ..................................................................................................... 18
           2.2.3.1. Via web .................................................................................................. 18
           2.2.3.2. Via certsrv ............................................................................................ 18
       2.2.4. Revoke cert ..................................................................................................... 19
           2.2.4.1. Via certsrv ............................................................................................ 19
1. Introduction

A primary security control in a PKI is how the private keys are stored and managed, especially when it concerns 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 help in cryptographic operations.

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

It is highly recommended that a strong protection strategy is taken when using the BlackVault HSM, ensure that the BlackVault resides in a secure place, that the smart cards associated with the operators of the BlackVault are stored correctly, and that everything is properly backed up.

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 HSM with the Microsoft CA.

The benefits of using an 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 Card Set
- BlackVault HSM Setup CD
- A client computer that has a supported Operating System installed.

Additionally, the BlackVault must be Initialized and Configured properly (see section 6.3 and 6.4 of 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 (included on the Setup CD)

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 as User operator
3. Add Microsoft Active Directory Certificate services
   a. In the Server manager window click on “Add roles and features”
   b. The Add Roles and Features Wizard will appear. Press Next to continue
   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. The next screen is Selection of Server Roles. Select “Active Directory Certificate Services” and press Next.
f. Next is Select Features screen. Press next.

![Select features](image)

- Select one or more features to install on the selected server.
- Description: NET Framework 3.5 combines the power of the NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

![Add Roles and Features Wizard](image)

- Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS), and smart card logon.

- Things to note:
  - The name and domain settings of this computer cannot be changed after a certification authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.

![Active Directory Certificate Services](image)

- Before you begin:
  - Installation Type
  - Server Name
  - Server Roles
  - Features
  - AD CS
  - Role Services
  - Confirmation
  - Results

- Description:
  - Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS), and smart card logon.
  - Things to note:
    - The name and domain settings of this computer cannot be changed after a certification authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.

- Next is Select Features screen. Press next.

- In the description of Active Directory Certificate Services screen press Next.
h. On the Select role service page select the role services required for this installation, (select at least Certification Authority) and press next

i. On the Confirmation page press Install.
j. After the wizard has finished installing, on the Results page press Close

2.1.2. Configuring the Active Directory Certificate Authority


The AD CS Configuration Window will now be displayed. Press Next to continue.
b. On the role Services page, select the roles you wish to configure (choosing at least Certificate Authority) and press Next.
c. On the Setup Type page, select standalone CA and press Next

d. On the CA Type page, choose CA type (root ca for this example) and press Next
e. On the Private Key page, select “Create a new private key” and press Next

![Private Key page](image1)

f. On the Cryptography page,
i. In the “Select a cryptographic provider:” drop down menu, select one of the three Engage CSPs, ECDSA_P256#Engage BlackVault Cryptography Provider, ECDSA_P384#Engage BlackVault Cryptography Provider, or RSA_SIGN#Engage BlackVault Cryptography Provider

ii. In the Key Length drop down menu, select the appropriate key length.

iii. Select a proper key length, and a proper hash algorithm, then press Next.

iv. On the CA name page, enter in the Common name, and the Distinguished name in the appropriate fields then press Next.
h. On the Validity Period page, select the how long you want the CA to remain valid, then press Next.

![Validity Period](image1)

i. 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.

![CA Database](image2)
j. On the confirmation screen, review the configuration, then press Configuration.

k. The configuration will now begin, once the results screen shows up, press Close to complete the process.
2.2. Using MSCA

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

2.2.1. Import CSR

2.2.1.1. Via web

1. Open a Web browser.
2. Open https://servername/certsrv, where servername is the name of the server hosting the CA Web enrollment pages.
3. Click Request a certificate.
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.
   a. NOTE: The first option, create and submit a request to this CA cannot be chosen due to the BlackVault 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:
   o If the Certificate Pending Web page appears, see Check on a Pending Certificate Request for the procedure to check on a pending certificate.
   o If the Certificate Issued Web page appears, click Install this certificate.

2.2.1.2. Via certsrv

1. In the Start Menu, under administrative tools click on Certification Authority
2. Left Click the CA from the pool you wish to request a certificate from
3. On 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

2.2.2. Issue certificate

2.2.2.1. Via certsrv

1. In the Start Menu, under administrative tools click on Certification Authority
2. In the console Tree click Pending Requests
3. In the details pane, left click the certificate you want to revoke.
4. On the Action menu, point to All Tasks, and click Issue
2.2.3. Export cert

2.2.3.1. Via web

1. In Internet Explorer, connect to https://<servername>/certsrv, where <servername> is the name of the computer running the CA Web Enrollment role service.
2. Click **Download a CA certificate, certificate chain, or CRL**.
3. Click the encoding method that you want to use for the CRL, **DER** or **Base 64**.
4. Do one of the following:
   - Click **Download CA certificate**.
   - Click **Download CA certificate chain**.
   - Click **Download latest base CRL**.
   - Click **Download latest delta CRL**.
5. When the **File Download** dialog box appears, click **Save**. Select a folder on your computer to store the .crl file, and then click **Save**.
6. Open Windows Explorer and locate the .crl file you just saved.
7. Right-click the .cer or .crl file and click **Install Certificate** or **Install CRL**, and then click **Next**.
8. When the Certificate Import Wizard opens, click **Automatically select the certificate store based on the type of certificate**.

2.2.3.2. 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 DER-encoded 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**.
2.2.4. Revoke cert

2.2.4.1. Via certsrv

1. In the Start Menu, under administrative tools click on 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