GlobalSign Integration Guide

GlobalSign Managed SSL (MSSL) and
Azure KeyVault

GlobalSign
GMO Internet Group

Introduction

This technical integration guide describes how to integrate the Microsoft Azure KeyVault platform with GlobalSign's Managed SSL (MSSL) service to provision SSL certificate to be accessed and utilized through the Microsoft Azure cloud platform.

GlobalSign Managed SSL (MSSL)

A Complete Enterprise SSL Solution. Managed SSL is a SaaS solution to reduce the effort, cost and time associated with managing enterprise SSL Certificates. The Managed SSL platform was designed around enterprise-specific security requirements and gives access to all types of SSL Certificates. It supports the enterprise's needs to host public websites as well as for non-public and internal servers. GlobalSign offers unique features and functionality that make it easy to manage your certificates no matter how large or distributed your organization.

A robust platform that allows Instant issuance of all types of SSL Certificates on-demand, including Organization Validated (OV), Extended Validation (EV), Wildcard, and Multi-domain, with options to add Subject Alternative Names (SANs).

For more information on MSSL, see https://www.globalsign.com/en/ssl/managed-ssl/

Microsoft Azure Key Vault

Secure key management is essential to protect data in the cloud. Use Azure Key Vault to encrypt keys and small secrets like passwords that use keys stored in hardware security modules (HSMs). For more assurance, import or generate keys in HSMs, and Microsoft processes your keys in FIPS 140-2 Level 2 validated HSMs (hardware and firmware). With Key Vault, Microsoft doesn't see or extract your keys.

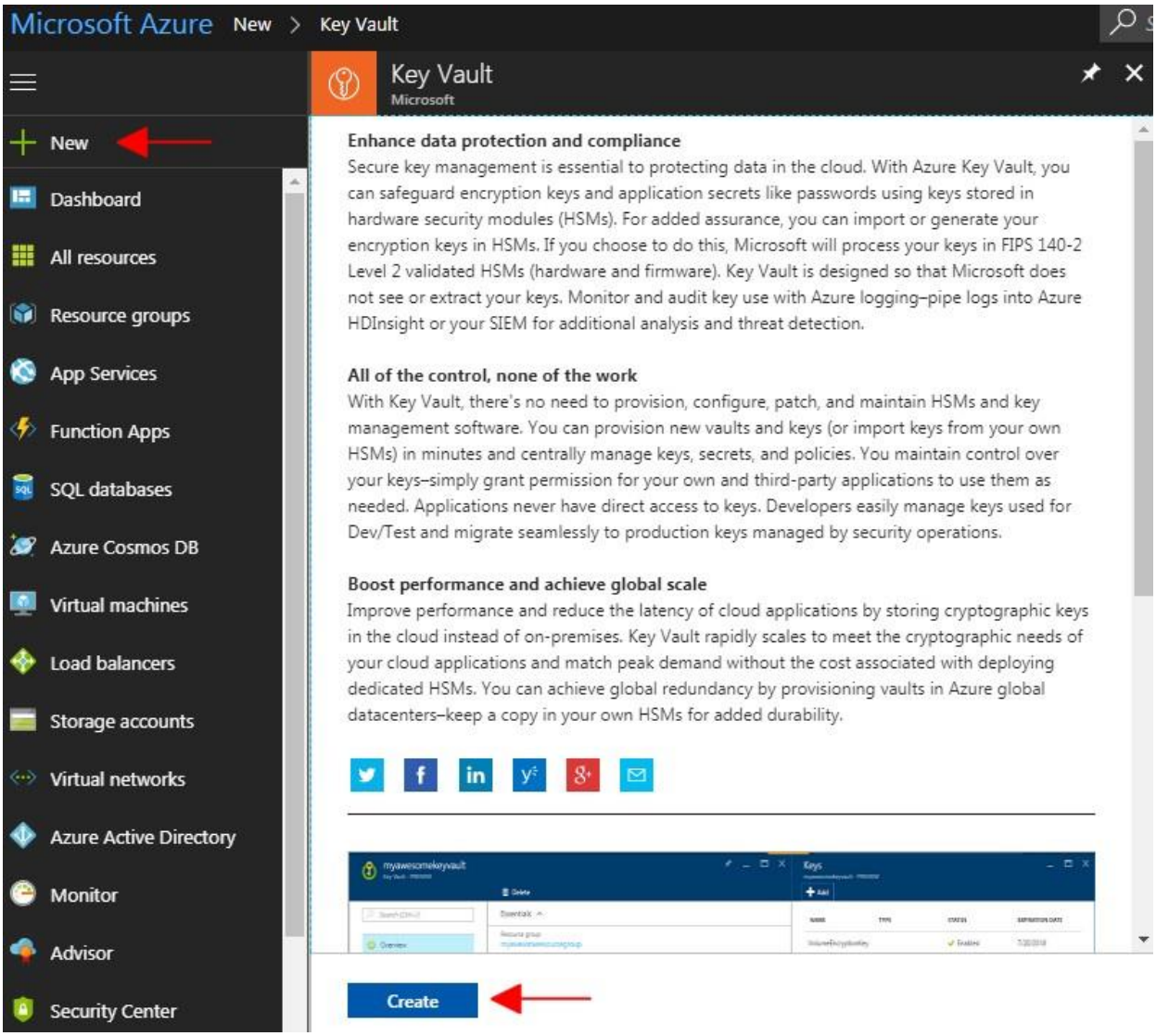
Provision new vaults and keys in minutes and centrally manage keys, secrets, and policies. You keep control over your keys—simply grant permission for your own and partner applications to use them as needed. Applications never have direct access to keys. Developers manage keys used for Dev/Test and seamlessly migrate to production the keys that are managed by security operations. Simplify and automate tasks related to SSL/TLS certificates—Key Vault enables you to enroll and automatically renew certificates from supported public Certificate Authorities.

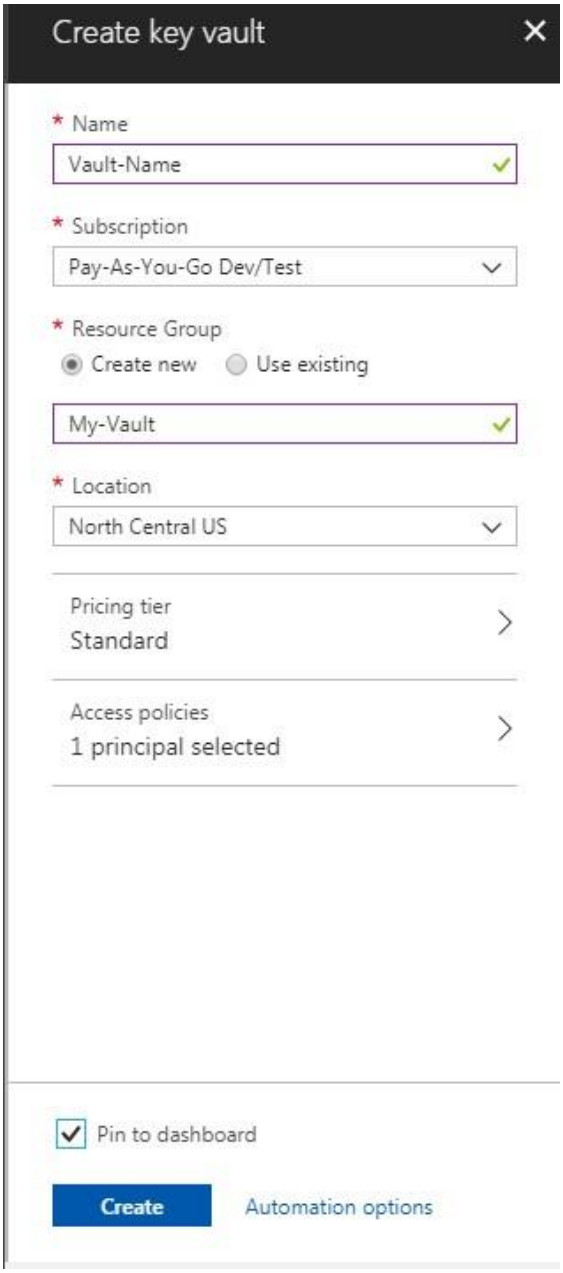
For more information on Azure KeyVault, see https://azure.microsoft.com/en-us/services/key-vault/

GlobalSign Contact Information

GlobalSign Americas Tel: 1-877-775-4562 www.globalsign.com sales-us@globalsign.com	**GlobalSign EU** Tel: +32 16 891900 www.globalsign.eu sales@globalsign.com	**GlobalSign UK** Tel: +44 1622 766766 www.globalsign.co.uk sales@globalsign.com
GlobalSign FR Tel: +33 1 82 88 01 24 www.globalsign.fr ventes@globalsign.com	**GlobalSign DE** Tel: +49 30 8878 9310 www.globalsign.de verkauf@globalsign.com	**GlobalSign NL** Tel: +31 20 8908021 www.globalsign.nl verkoop@globalsign.com

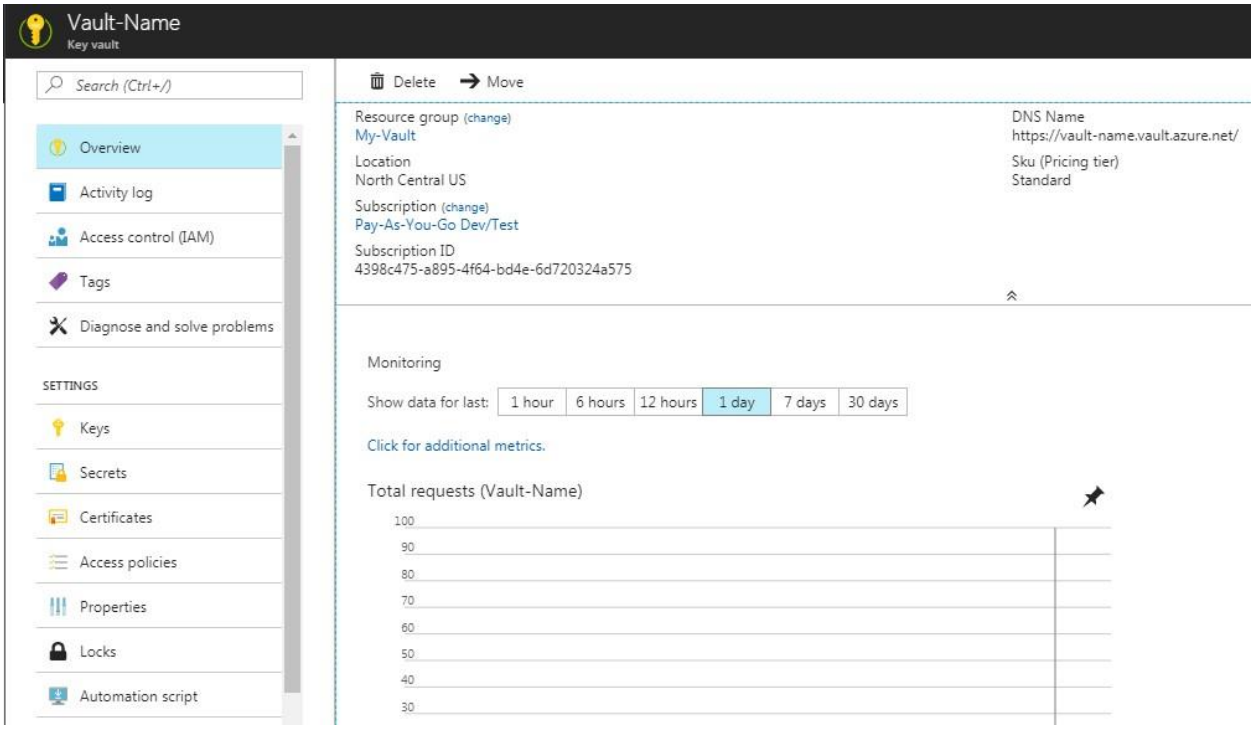
Once logged into the Azure portal, if you do not have a Key Vault setup yet or would like to create a new one click on the “New” tab on the left hand side menu and choose “Key Vault” icon. (Note: If it does not auto populate you can use the search bar and it will pop up).



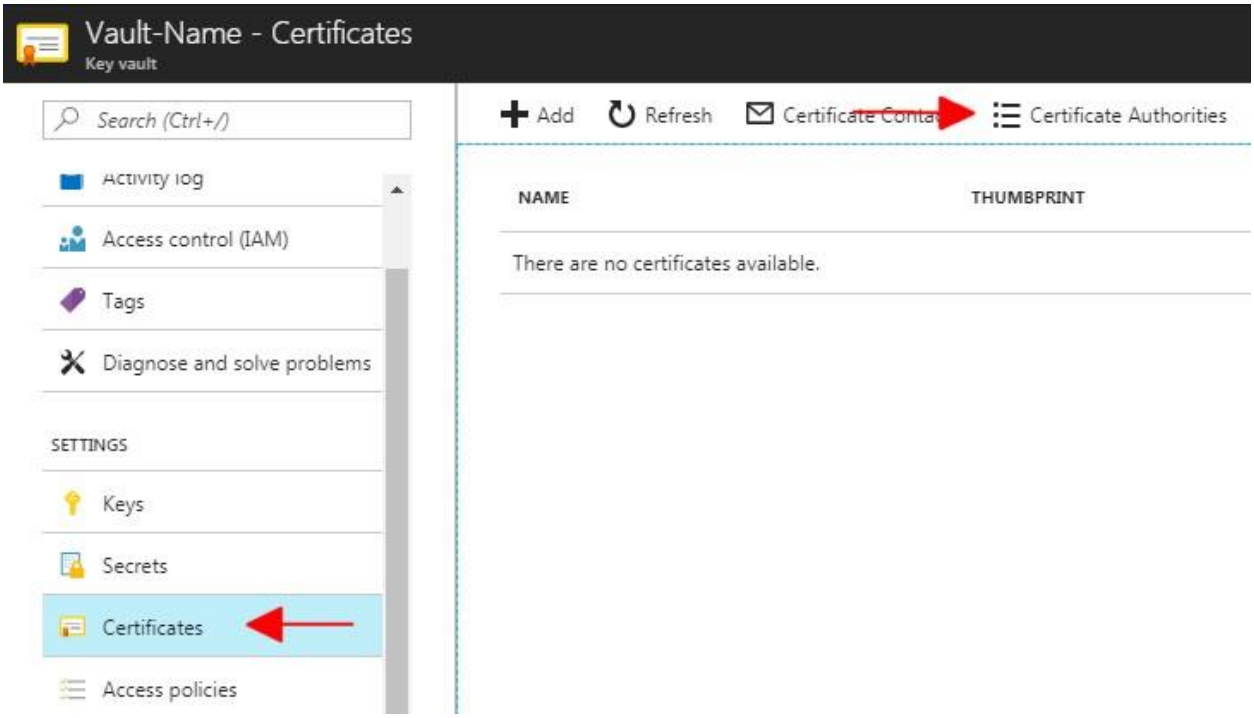


Now you will want to Name your key vault. Once named choose your subscription preferences, resource group (new or existing), location, pricing tier and the vaults access policies. Once complete, click the “Create” button.

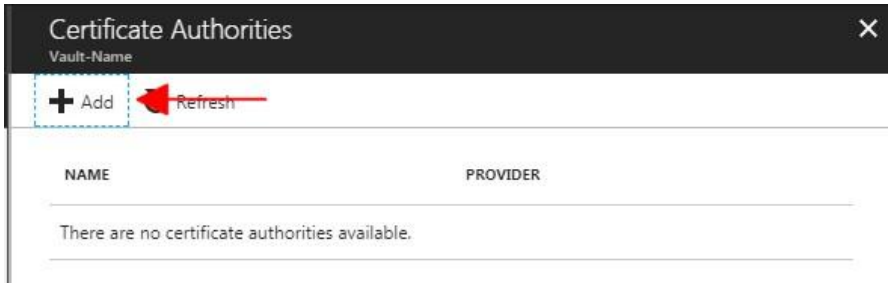
Your vault will now be created and you will be taken to an overview of its configuration.



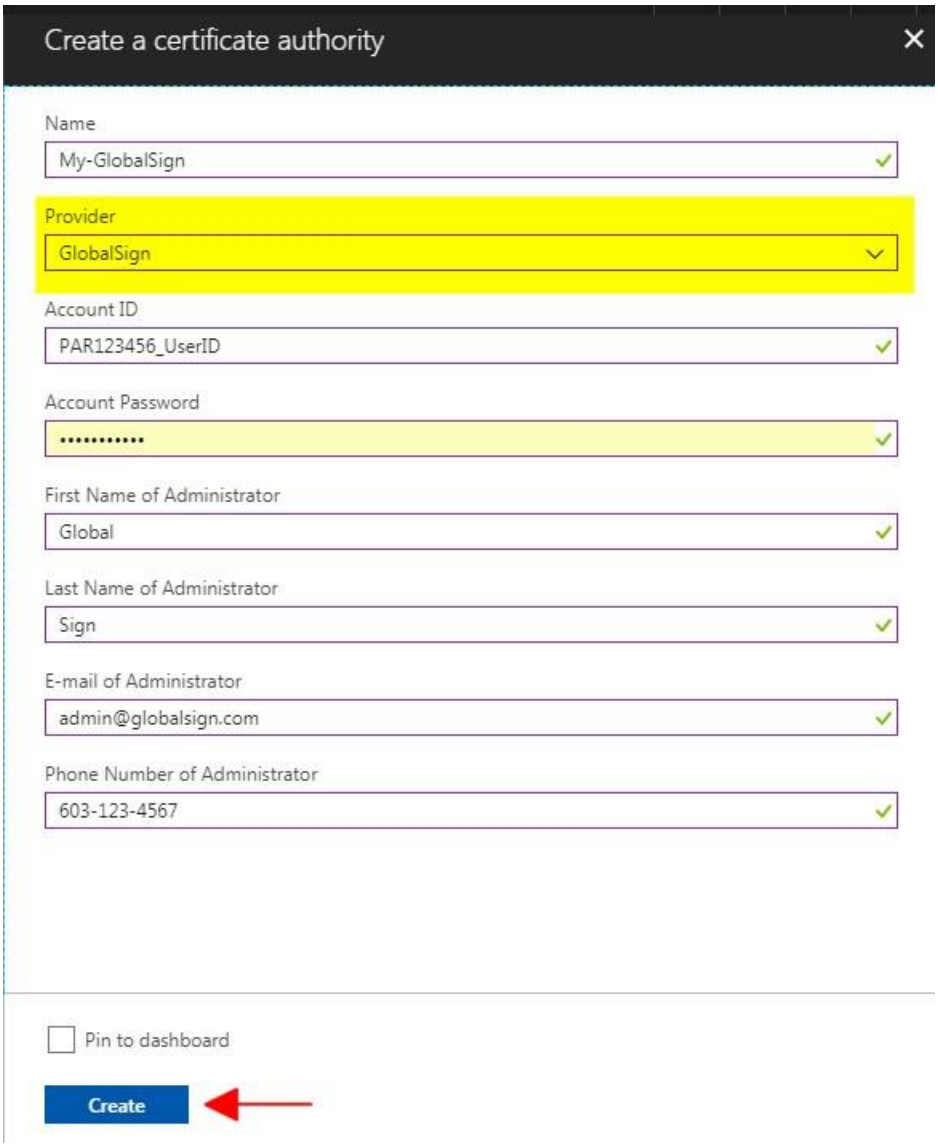
Next you will want to create a GlobalSign Certificate Authority for the vault to access. From the left side menu choose “Certificates”. A menu will open and on the upper right hand side choose “Certificate Authorities”.



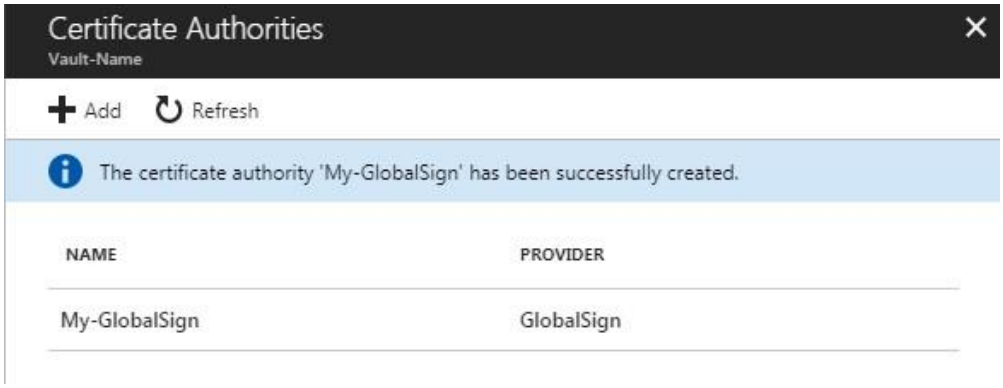
Under the Certificate Authorities menu select “Add”.



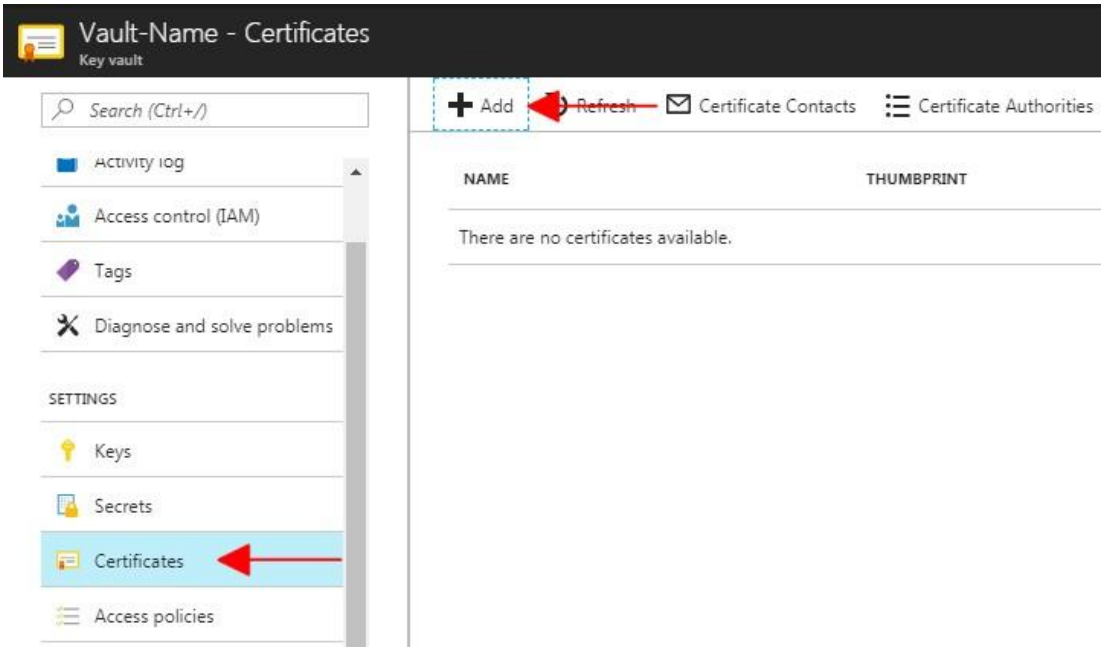
Once you name your certificate authority accordingly, you will want to click on the “Provider” tab and from the drop down menu select “GlobalSign”. The menu will then populate fields for you to enter your GlobalSign account information.



You should then get notification that the certificate authority has been successfully created.



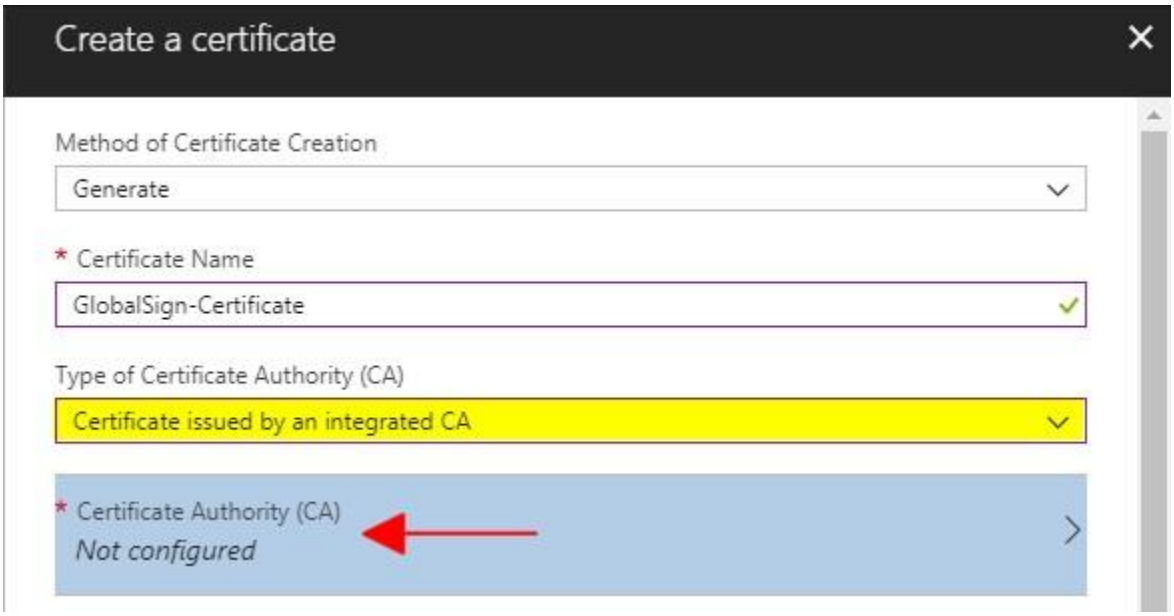
Next step is to add a new certificate to the vault. To do this, click on the “Certificates” tab on the left hand side menu and then click “Add”.



Here you will want to choose “Generate” as the method of certificate generation and then specify a certificate name. (Note: This is a friendly name that it will be referred to with in the vault, it is not the common name of the actual certificate.)

You will then want to select “Certificate issued by an integrated CA” from the “Type of Certificate Authority (CA)” drop down menu.

Then click the “Certificate Authority (CA) *Not Configured*” tab.

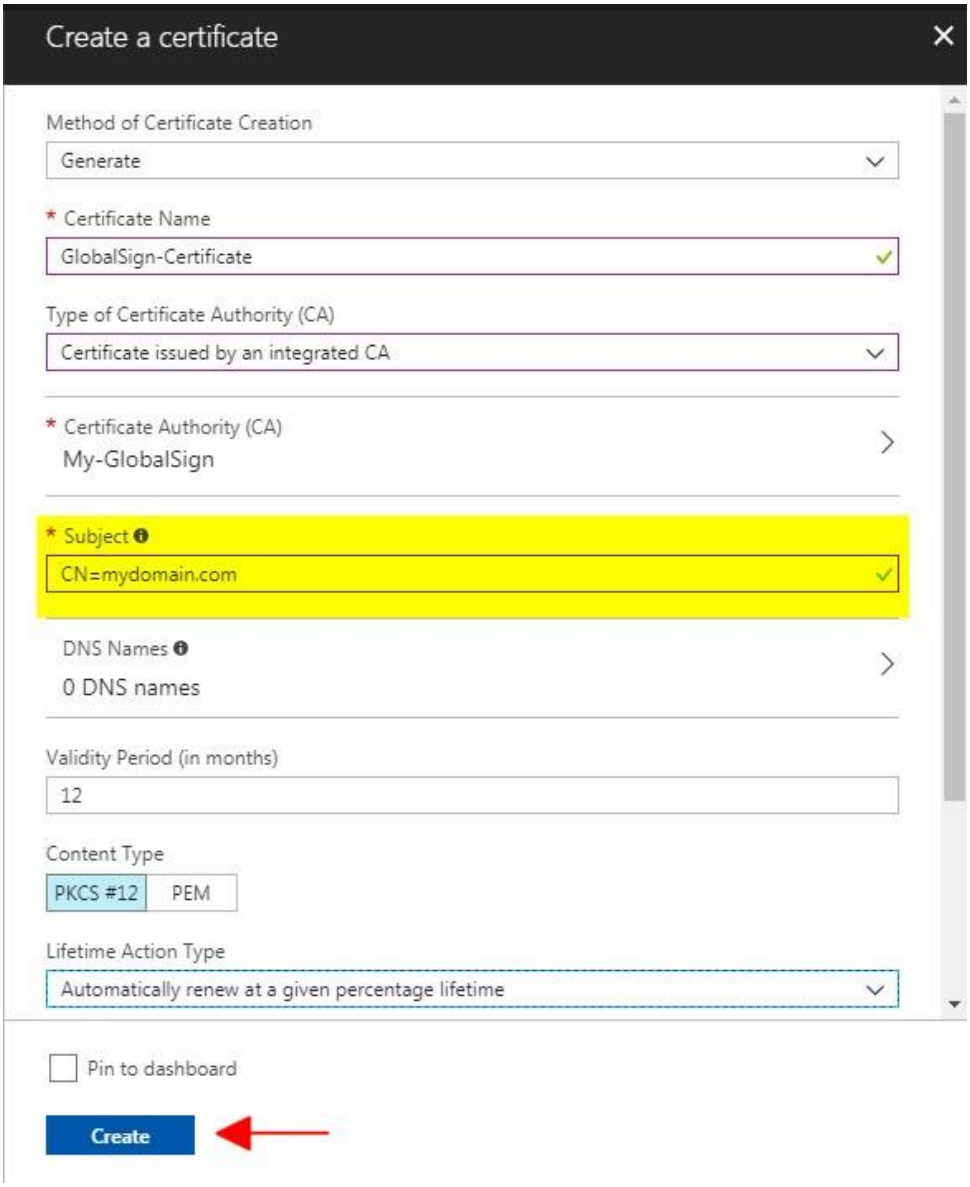


Next you will want to select the GlobalSign Certificate Authority that you created. This will take you back to the Create a certificate form.

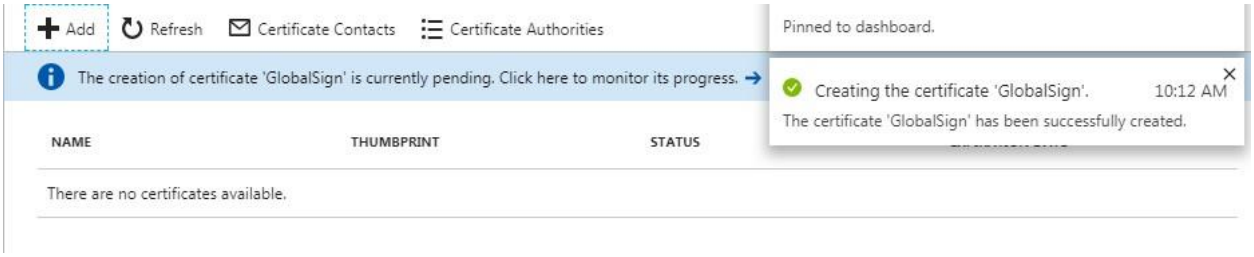
The final requirement is the “Subject” field. This is where you will enter the common name for the certificate you are requesting (Format: CN=commonname.com).

There are additional fields which are optional:

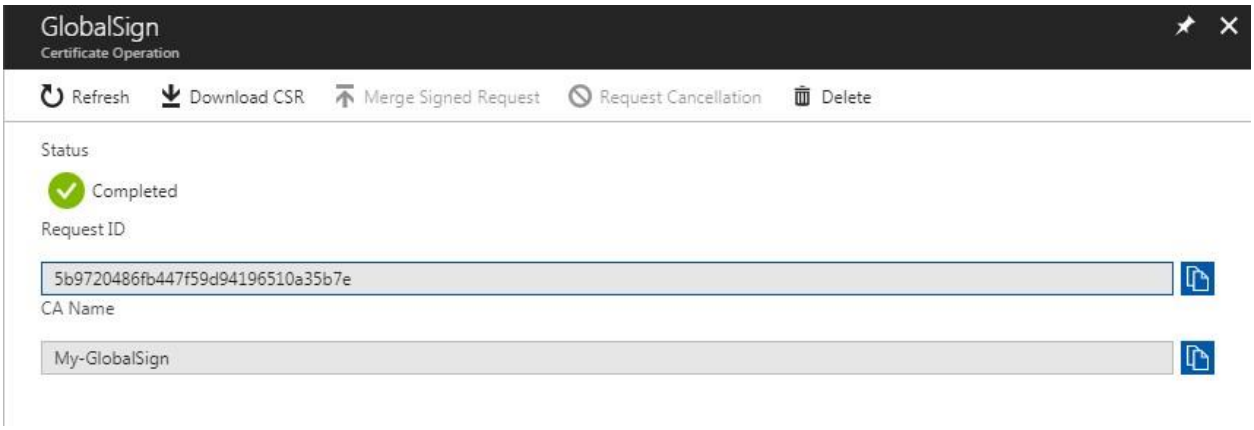
- DNS Names – Where add additional Subject Alternative Names (SANs)
- Validity Period – To select how long the certificate is valid for in month designation
- Content Type
    - PKCS#12 – private public key pair
    - PEM – public key
- Lifetime Action Type – Set certificate renewals or renewal reminders
- Advanced Policy Configuration – Add additional EKUs and set advanced key features



A pop up in the right corner will confirm the certificate is being created. You can also click on the blue information bar to monitor the generation process.



Status completed confirms that the certificate has been issued and stored in the vault.



Under the menu bar, go to “Certificates” to see your list of issued Certificates. You are now able to utilize the certificate through the Azure platform.