Garantir

GaraSign Azure Key Vault Integration

Table of Contents

Preface

Document Information

Title	GaraSign Azure Key Vault Integration
Initial Release	2021

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. Without limiting the rights under the copyright reserved above, no part of this publication may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without the prior written permission of Garantir.

Disclaimer

Garantir makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Garantir reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon Garantir to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be without error or otherwise perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

Please send any constructive comments on the contents of this document to the following email address: support@garantir.io

Document Overview

GaraSign can integrate with multiple different HSMs and can do so simultaneously. This document describes how to integrate GaraSign with Azure Key Vault as its key container. The same implementation may also be used for equivalent integrations such as Azure Managed HSM.

Intended Audience

All products produced by Garantir are designed to be installed, configured, operated, and maintained by personnel with the necessary knowledge, skill, training, and qualifications to safely perform their duties. This document is intended for personnel responsible for architecting, engineering, installing, configuring, operating, and/or troubleshooting enterprise signing solutions. It is assumed that the readers of this document and the users of its content are proficient with:

- Basic networking concepts
- Security concepts including, but not limited to, authentication, authorization, digital signatures, and logging
- Azure configuration and usage

Additionally, it is strongly recommended that readers of this document first read the GaraSign datasheet.

GaraSign Overview

GaraSign is a flexible enterprise cryptographic signing platform that carefully balances security and performance. Unlike most solutions today that require clients to upload the data to be signed to a central location, GaraSign is designed as a remote signing platform. As shown in Figure 1 below, GaraSign clients first hash the data to sign and then send the computed hash value over a secure channel to the GaraSign server for signing. Using this approach, no matter how large the data is, the data sent over the network is minimal which allows for optimum performance. Behind the GaraSign server sits one or more cryptographic tokens (e.g., HSMs, key managers, etc.) that GaraSign can offload signature processing to once the appropriate authentication and authorization checks have been made. By placing the GaraSign server between the client and the back-end HSM, not only is performance significantly increased, other enterprise features such as advanced authentication, enterprise logging, email notifications, and more are enabled. As an additional benefit, the GaraSign server acts as a buffer between your end clients and your HSMs, which not only significantly reduces the integration complexities that your clients must deal with but also helps to shield your cryptographic keys from attack and misuse.

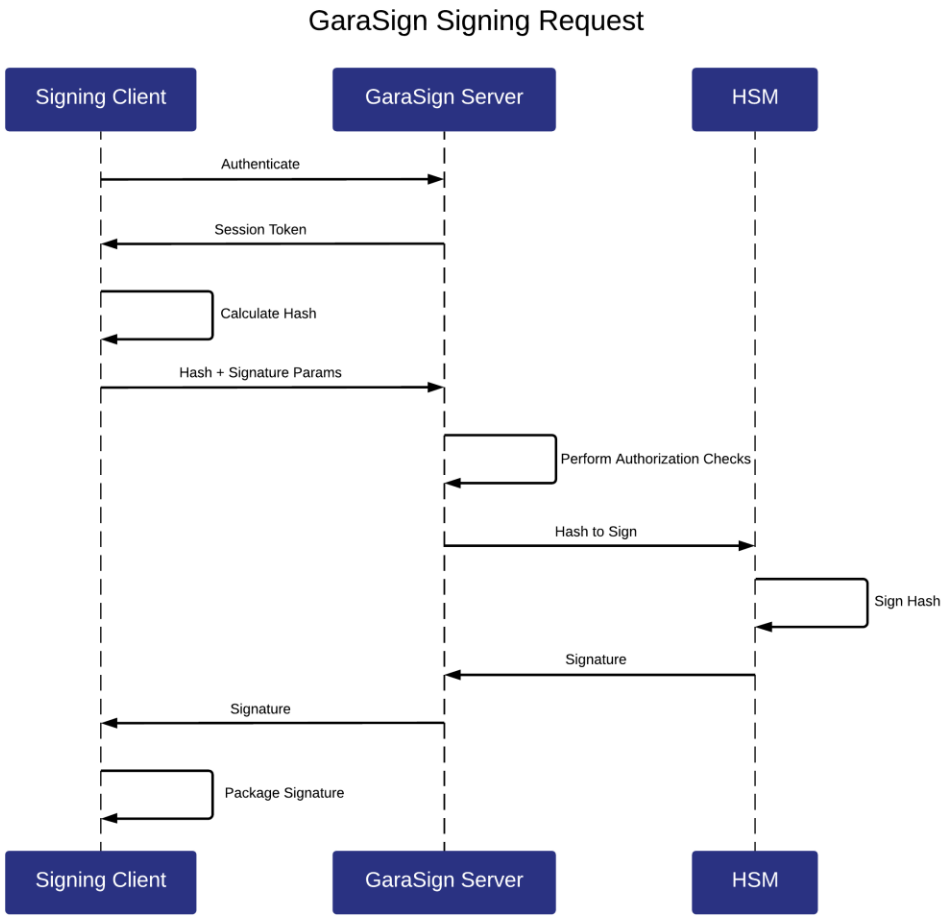


Figure 1 - GaraSign Signing Request

Note: while this document makes mention of REST servers, GaraSign is designed to sit on-premise in your network and/or in your virtual private cloud. Garantir does **not** have access to any of your infrastructure and does **not** control your cryptographic keys.

Azure Key Vault Integration

Integrating GaraSign with Azure Key Vault is done by performing the steps outlined in the following sections. Once complete, Azure Key Vault can be used like any other key container in GaraSign to create keys, generate certificate signing requests (CSRs), import certificates, sign and decrypt data, and more.

Prerequisites

The following prerequisites must be satisfied before configuring the Azure Key Vault key container in GaraSign.

1. Create the Key Vault in Azure
   Note: GaraSign will always attempt to generate keys as HSM-protected, regardless if the type of vault is generated as Vault or Managed HSM
2. Create an Entra ID Service Principal with the following permissions on the Key Vault:
   a. (**Required**) Keys: all operations (key management and crypto operations)
   b. (Optional) Certificates: all operations. Note: GaraSign defaults to storing certificates in its database.
   c. (Optional) Secrets: all operations. Note: only needed for secrets management use cases.
3. Ensure the GaraSign signing and admin servers have network access to the Azure Key Vault
4. Create the Azure Key Vault key container in GaraSign

Details for steps 1 and 2 can be found on the Azure portal.

The rest of this section focuses on step 4 – creating the key container in the GaraSign Administrative Console.

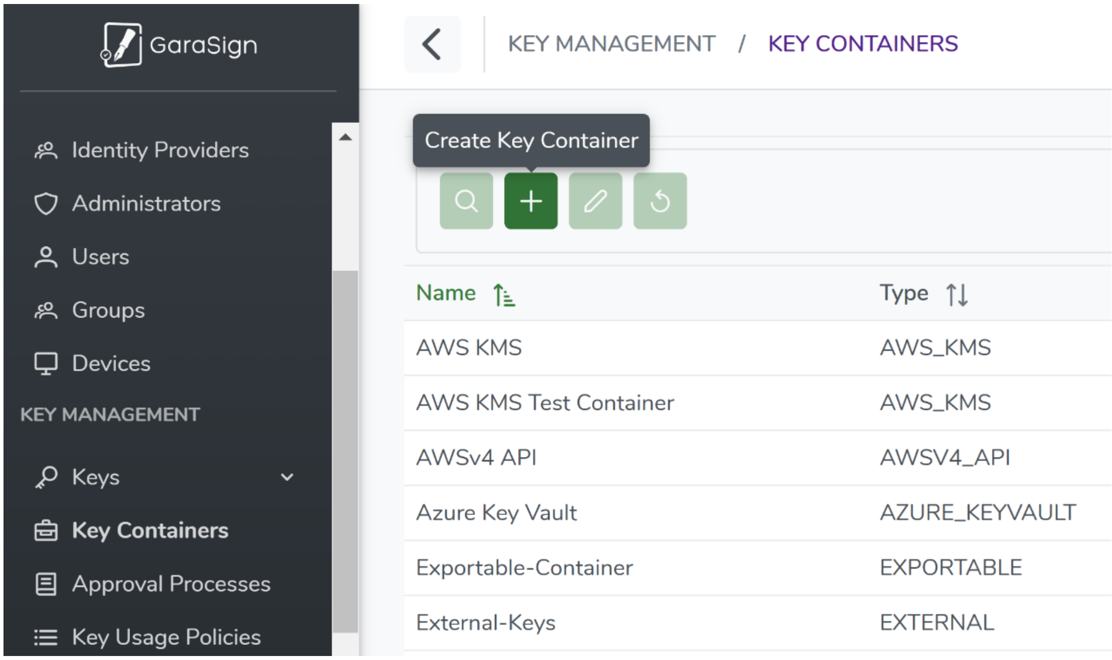
Create Azure Key Vault Key Container

The Azure Key Vault Key Container can be configured within GaraSign either via the Administrative Web Console, or via the Command Line Utility.

Administrative Web Console

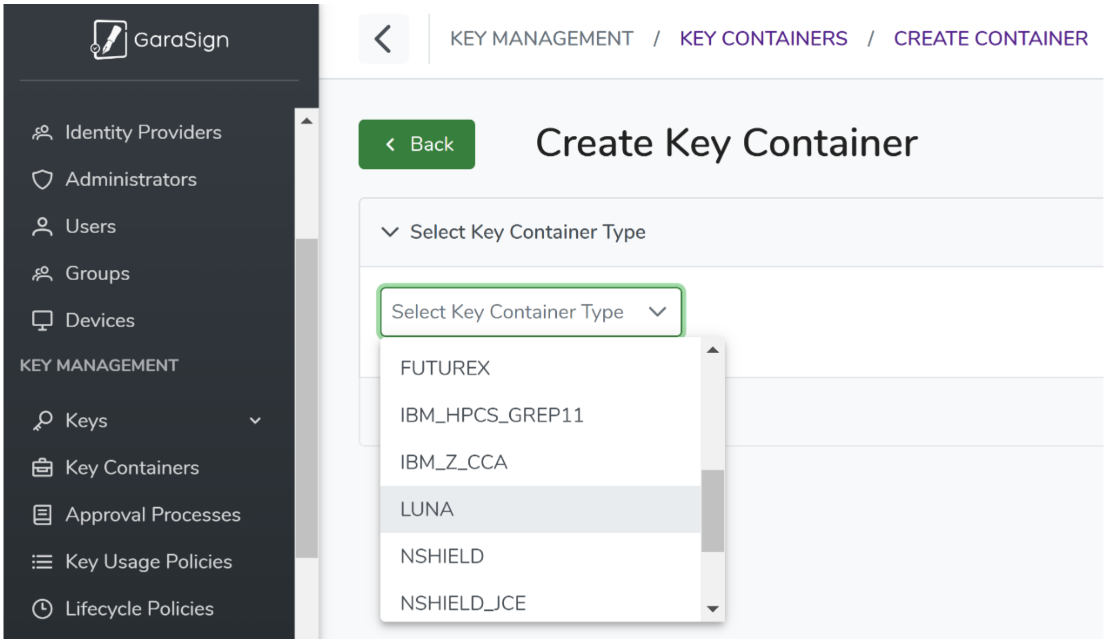
Follow the steps from your GaraSign Admin User Guide to launch the GaraSign Administrative Web Console and login with Key Container Administrator rights. Once logged in, perform the following steps:

1. On the left-hand navigation click on *Key Containers* under *Key Management*.
2. On the right-hand page, click the + button above the table to create a new key container.

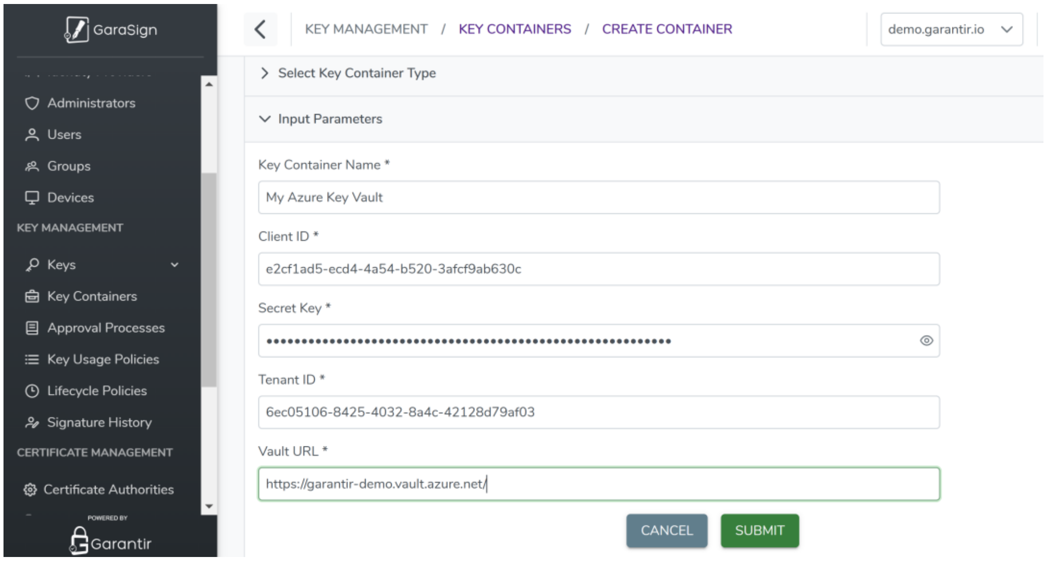


Name	Type
AWS KMS	AWS_KMS
AWS KMS Test Container	AWS_KMS
AWSv4 API	AWSV4_API
Azure Key Vault	AZURE_KEYVAULT
Exportable-Container	EXPORTABLE
External-Keys	EXTERNAL

3. From the dropdown menu, select *AZURE_KEYVAULT* as the *Key Container Type*



4. Enter a desired name for the key container. This value can be any value you like.
5. Enter the Service Principal's Client ID.
6. Enter the Service Principal's Secret Value.
7. Enter the Tenant ID.
8. Enter the Vault URL.
9. Click Submit to create the key container. The process may take several moments to connect to your Azure Key Vault. Please be patient.



Key Container Name *
My Azure Key Vault

Client ID *
e2cf1ad5-ecd4-4a54-b520-3afcf9ab630c

Secret Key *
••

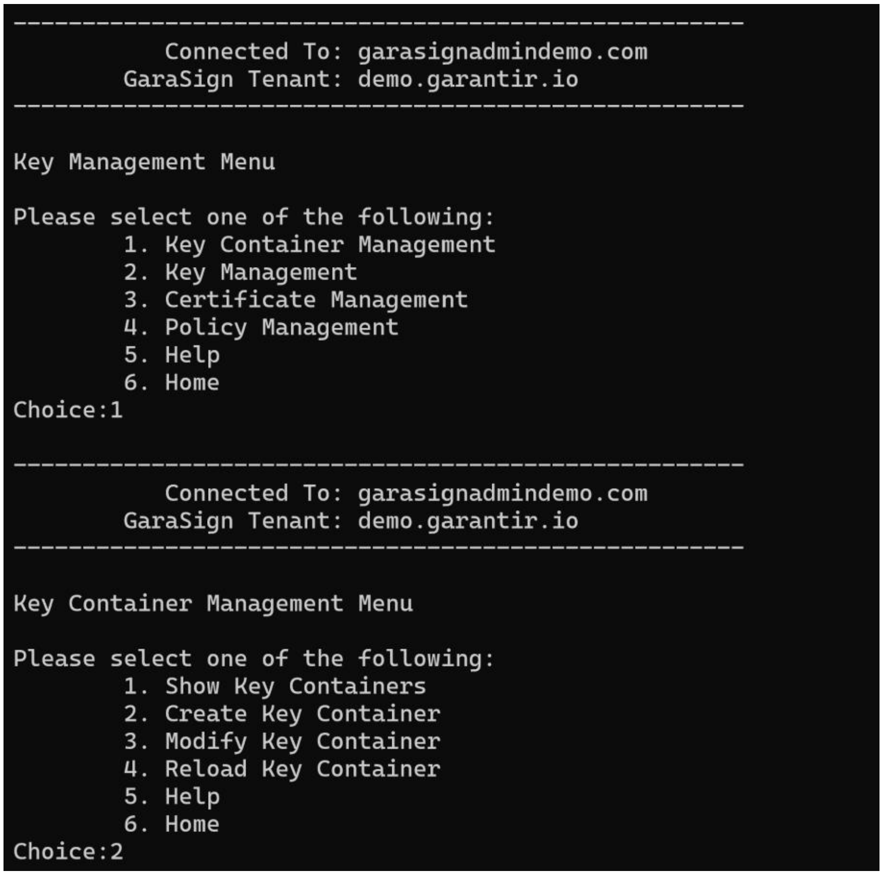
Tenant ID *
6ec05106-8425-4032-8a4c-42128d79af03

Vault URL *
https://garantir-demo.vault.azure.net/

Command Line Utility

Follow the steps from your GaraSign Admin User Guide documentation to launch the GaraSign Administrative Console and login with Key Container Administrator rights. Once logged in, perform the following steps:

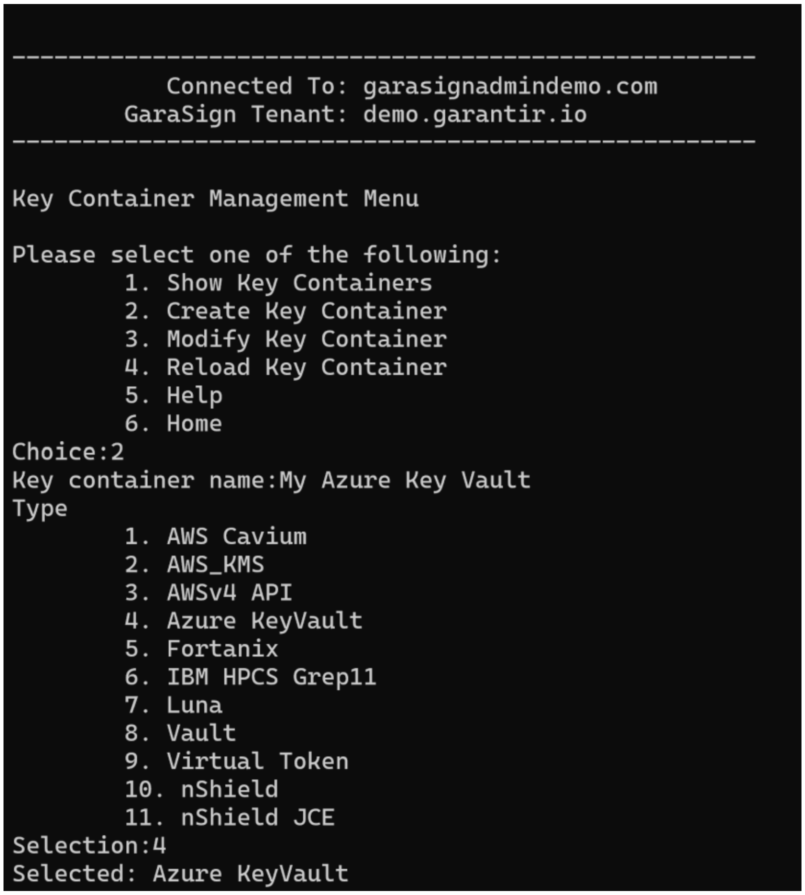
1. From the *Main Menu* select *Key Management* and then *Create Key Container*.



```
-----------------------------------------------------
           Connected To: garasignadmindemo.com
        GaraSign Tenant: demo.garantir.io
-----------------------------------------------------

Key Management Menu

Please select one of the following:
        1. Key Container Management
        2. Key Management
        3. Certificate Management
        4. Policy Management
        5. Help
        6. Home
Choice:1

-----------------------------------------------------
           Connected To: garasignadmindemo.com
        GaraSign Tenant: demo.garantir.io
-----------------------------------------------------

Key Container Management Menu

Please select one of the following:
        1. Show Key Containers
        2. Create Key Container
        3. Modify Key Container
        4. Reload Key Container
        5. Help
        6. Home
Choice:2
```

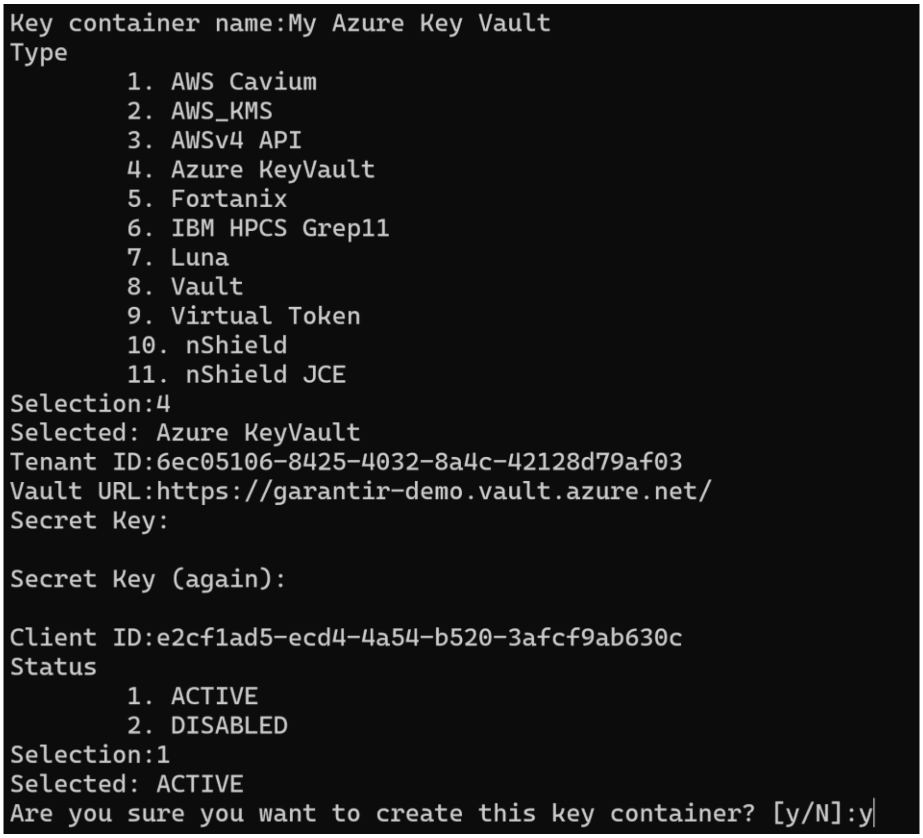
2. Give the key container a name. Note: this name must be globally unique amongst all key containers in your GaraSign deployment.

3. For *Key Container Type* choose *Azure Key Vault.*



```
-----------------------------------------------------
           Connected To: garasignadmindemo.com
        GaraSign Tenant: demo.garantir.io
-----------------------------------------------------

Key Container Management Menu

Please select one of the following:
        1. Show Key Containers
        2. Create Key Container
        3. Modify Key Container
        4. Reload Key Container
        5. Help
        6. Home
Choice:2
Key container name:My Azure Key Vault
Type
        1. AWS Cavium
        2. AWS_KMS
        3. AWSv4 API
        4. Azure KeyVault
        5. Fortanix
        6. IBM HPCS Grep11
        7. Luna
        8. Vault
        9. Virtual Token
        10. nShield
        11. nShield JCE
Selection:4
Selected: Azure KeyVault
```

4. Enter the Tenant ID
5. Enter the Vault URL
6. Enter the Service Principal's Secret Value. You will be prompted for this twice.
7. Enter the Service Principal's Client ID.
8. Choose whether this key container is to be Active or Disabled. In most scenarios the container should be Active. Please see your GaraSign Administrative User Guide for more information.
9. At the confirmation prompt please check that the information you provided is accurate. If it is, type *y* and then press Enter. Otherwise, just press Enter to cancel.



```
Key container name:My Azure Key Vault
Type
        1. AWS Cavium
        2. AWS_KMS
        3. AWSv4 API
        4. Azure KeyVault
        5. Fortanix
        6. IBM HPCS Grep11
        7. Luna
        8. Vault
        9. Virtual Token
        10. nShield
        11. nShield JCE
Selection:4
Selected: Azure KeyVault
Tenant ID:6ec05106-8425-4032-8a4c-42128d79af03
Vault URL:https://garantir-demo.vault.azure.net/
Secret Key:

Secret Key (again):

Client ID:e2cf1ad5-ecd4-4a54-b520-3afcf9ab630c
Status
        1. ACTIVE
        2. DISABLED
Selection:1
Selected: ACTIVE
Are you sure you want to create this key container? [y/N]:y
```

10. Once confirmed, the process may take several moments to connect to your Azure Key Vault. Please be patient.

Troubleshooting

If an error occurs during initialization or usage of the key container, the debug log file will contain useful information for troubleshooting. If the error occurred during key creation or destruction the log entry will be written to the administrative server's debug log file. If the error occurred during signing, encryption, or decryption, the log entry will be written to the signing server's debug log file. Common errors include:

- Firewall blocking network access to Azure Key Vault.
- Insufficient permissions given to the configured Service Principal.
- Incorrect or expired Secret Value for the given Service Principal.
- Incorrect Tenant ID or Vault URL specified.

Frequently Asked Questions

Are the keys exportable to the client?

No. The signing keys are generated as non-exportable and GaraSign does not expose any API to retrieve raw key bytes.

How is High Availability (HA) achieved with Azure Key Vault?

GaraSign makes use of the native Azure Key Vault client software, including its HA capabilities. Please see your Azure documentation for more information.

Does using Azure Key Vault slow down the process of signing?

No. Since GaraSign generates the hashes client-side, the network usage is minimal which results in fast signatures. No longer do customers have to choose between security and performance.