GaraSign Luna HSM Integration

Table of Contents

Preface

Document Information

Title	GaraSign Luna HSM Integration
Product Version	All

Trademarks

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 the Luna HSM as its key container. The Luna HSM may be used on-premise or hosted in the cloud using Safenet Data Protection on Demand (DPoD).

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
- Installing, configuring, and using the Luna HSM

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.

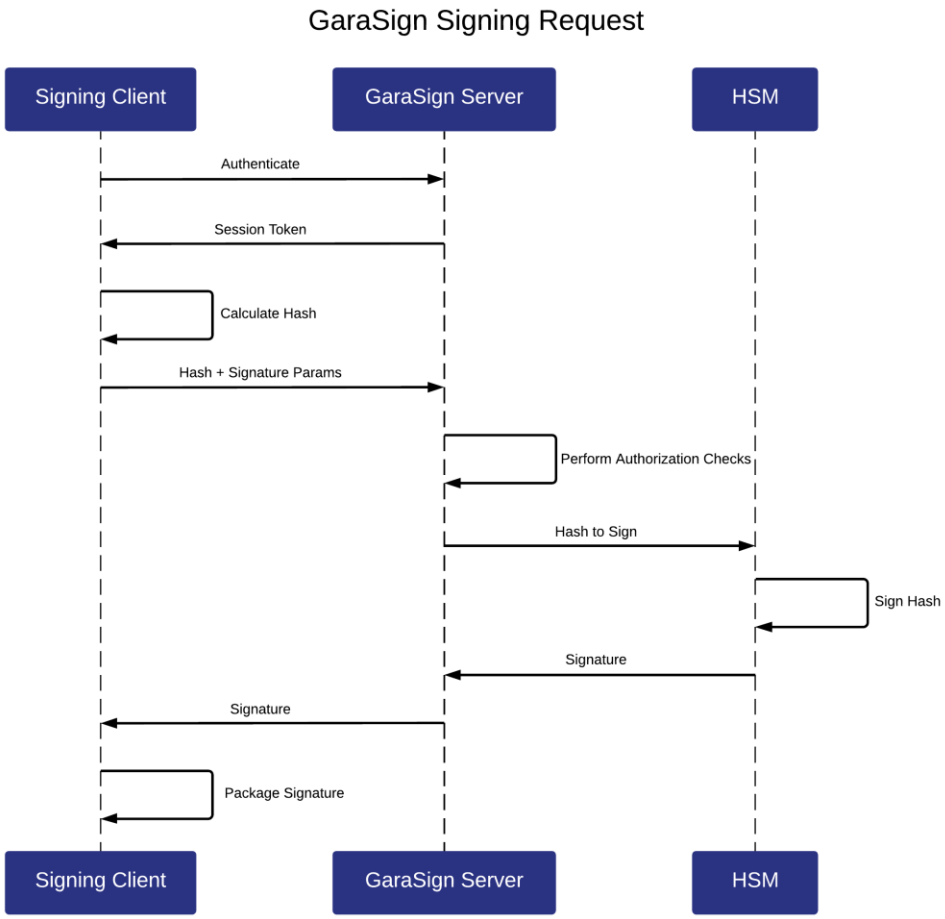


Figure 1 - GaraSign Signing Request

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.

Luna HSM Integration

Integrating GaraSign with the Luna HSM is done by performing the steps outlined in the following sections on each GaraSign Signing and Administration server. Once complete, the Luna HSM 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 Luna key container in GaraSign.

1. Install and configure the Luna Client including the Java (JSP) provider
2. Install the appropriate GaraSign software for the server type (i.e., GaraSign signing software for Signing Server and GaraSign admin software for Administration Server)
3. Copy LunaProvider.jar to Tomcat's lib folder
4. Ensure the LunaAPI library (LunaAPI.dll or LunaAPI.so) can be found on the PATH for the user that Tomcat runs as
5. Start (or restart) the Tomcat instances on the Signing and Administration servers

Details for step 1 can be found in your Luna HSM documentation. Please ensure connectivity to the Luna HSM using the Luna client tools prior to proceeding to the next step.

Details for step 2 can be found in your GaraSign documentation, although this is typically handled by your GaraSign professional services personnel.

For steps 3 and 4, the necessary Luna files can be found in the LunaClient/JSP/lib directory of your Luna HSM installation directory (e.g., C:\Program Files\SafeNet\LunaClient\JSP\lib on Windows).

The rest of this section focuses on step 5 – creating the key container in the GaraSign Administrative Console.

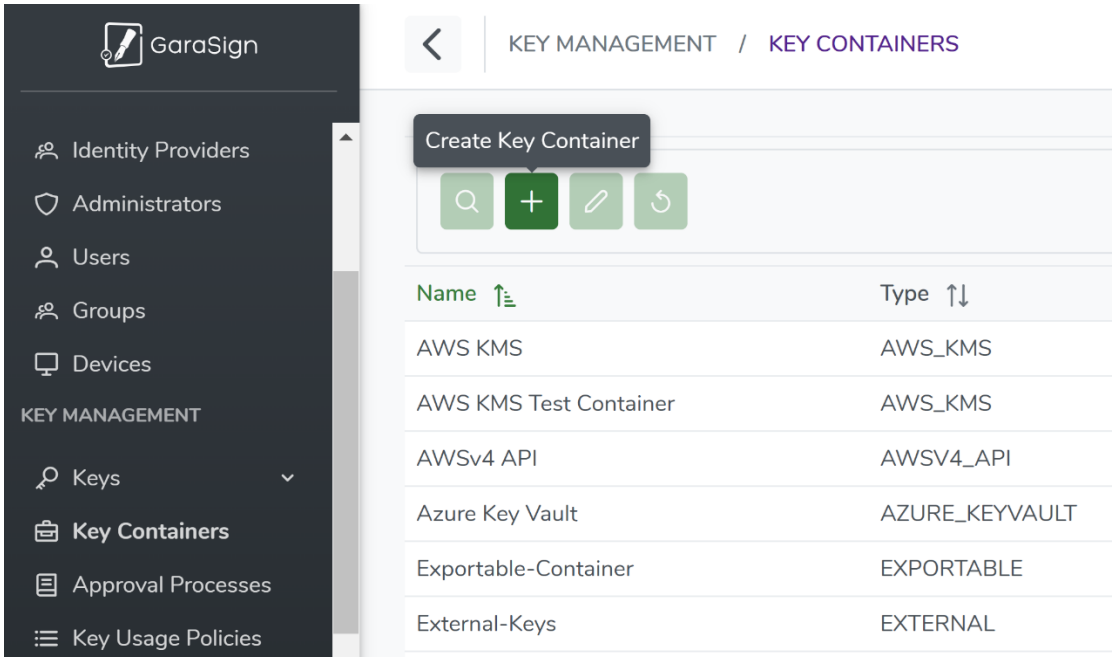
Create Luna Key Container

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

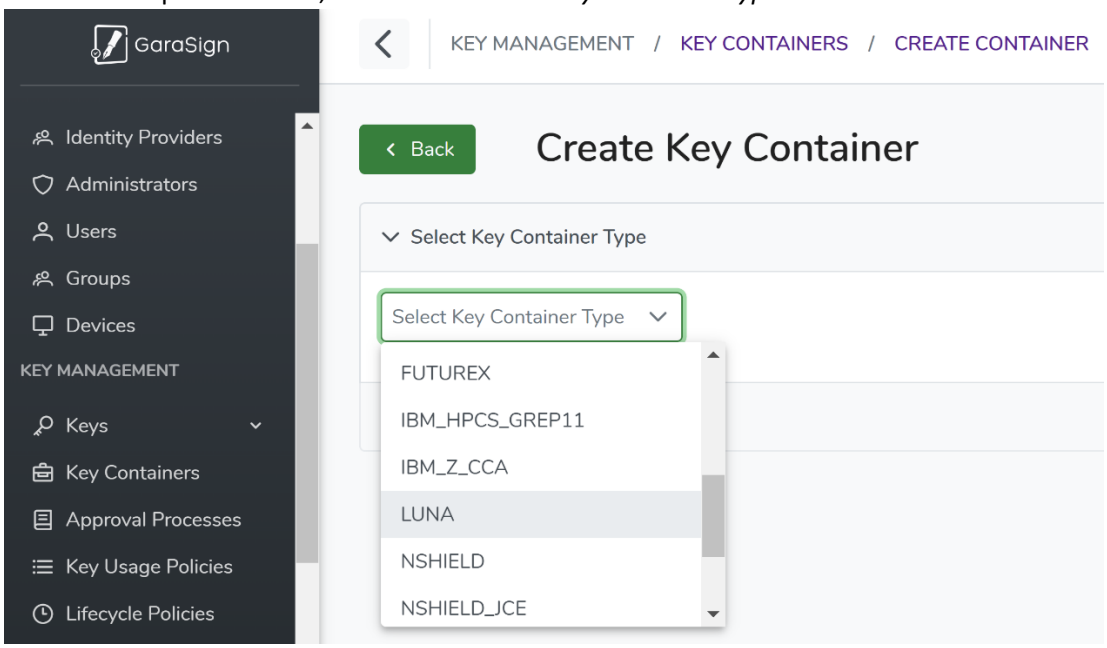
Administrative Web Console

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:

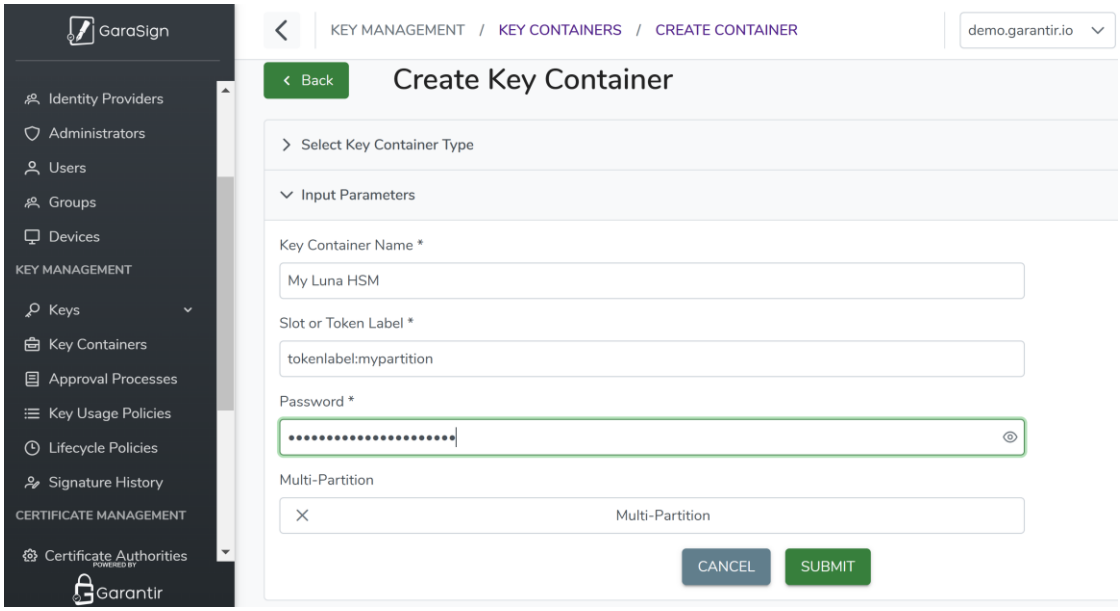
1. On the left-hand navigation click on *Key Containers* under *Key Management*.
2. On the right-hand page, click the + button above the table to create a new key container.



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



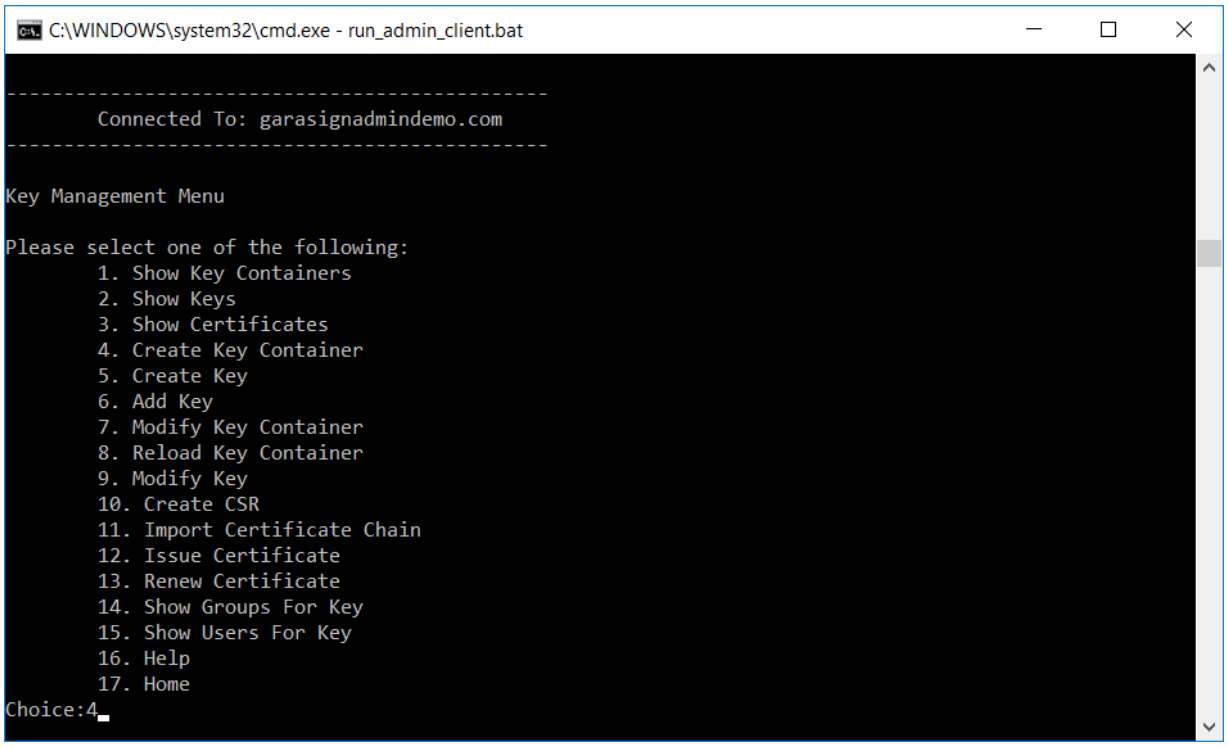
4. Enter a desired name for the key container. This value can be any value you like.
5. Enter the Slot or Token Label value in either *slot:<slot number>* or *tokenlabel:<label name>* format. Garantir strongly recommends using the Token Label wherever possible.
6. Enter the Partition's Crypto Officer Password.
7. If using multiple partitions, enable the Multi-Partition option.
8. Click Submit to create the key container. The process may take several moments to connect to your Luna HSM cluster. Please be patient.



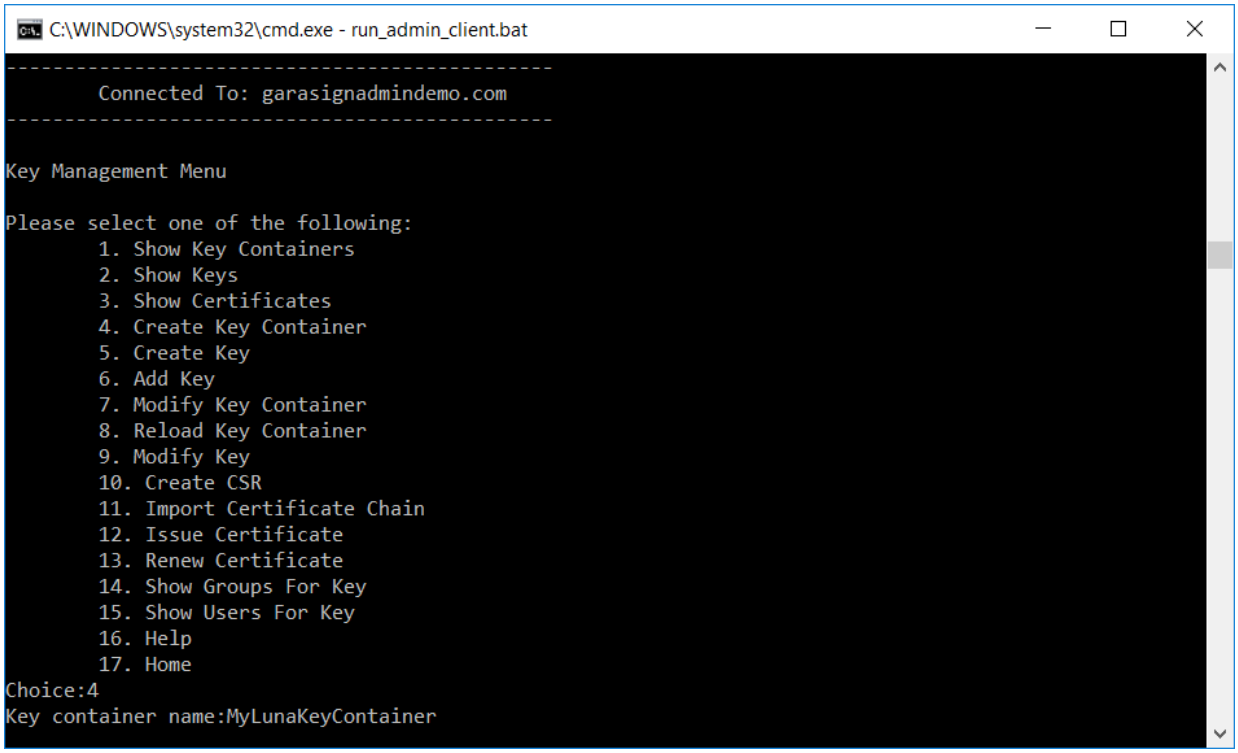
Command Line Utility

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:

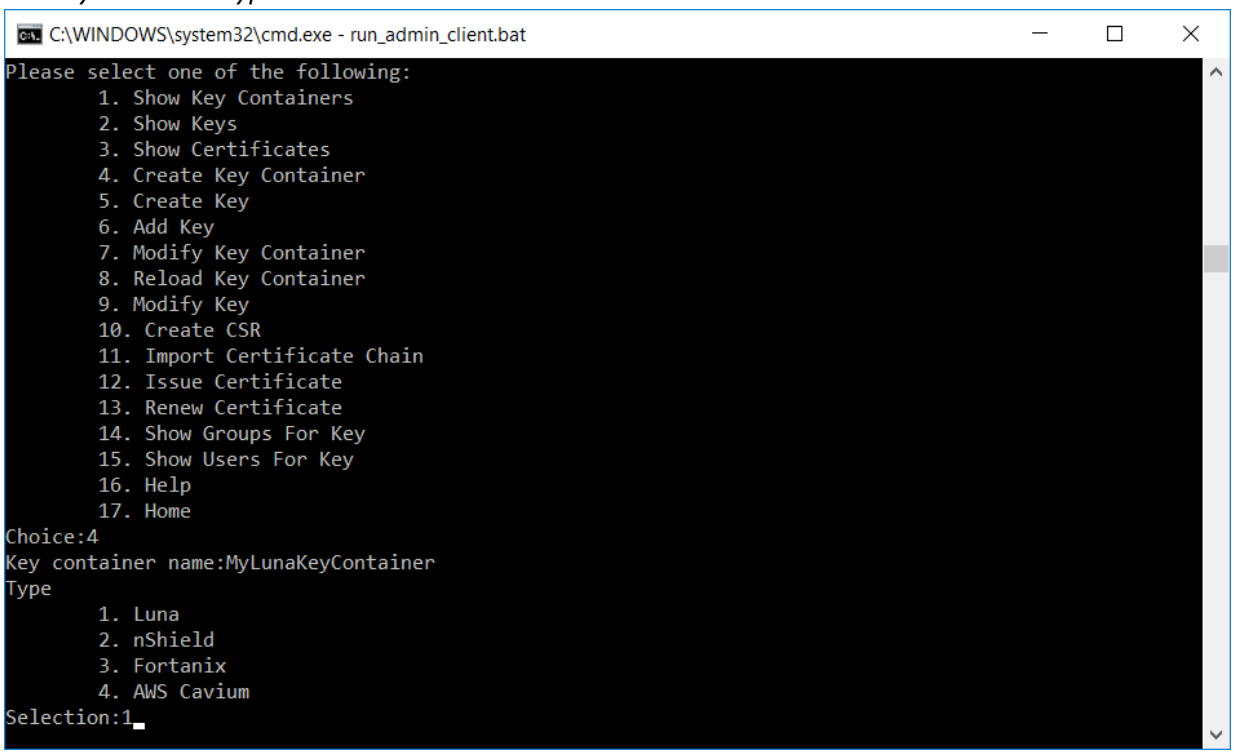
1. From the *Main Menu* select *Key Management* and then *Create Key Container*.



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

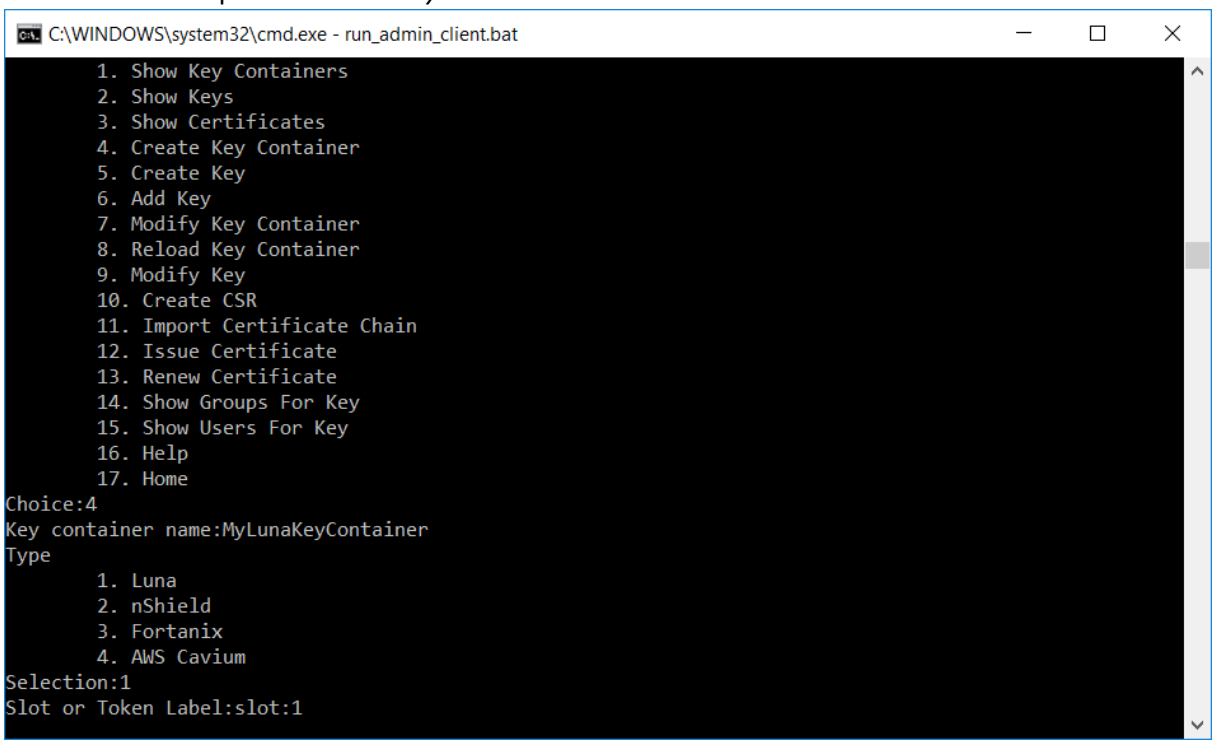


3. For *Key Container Type* choose the *Luna.*

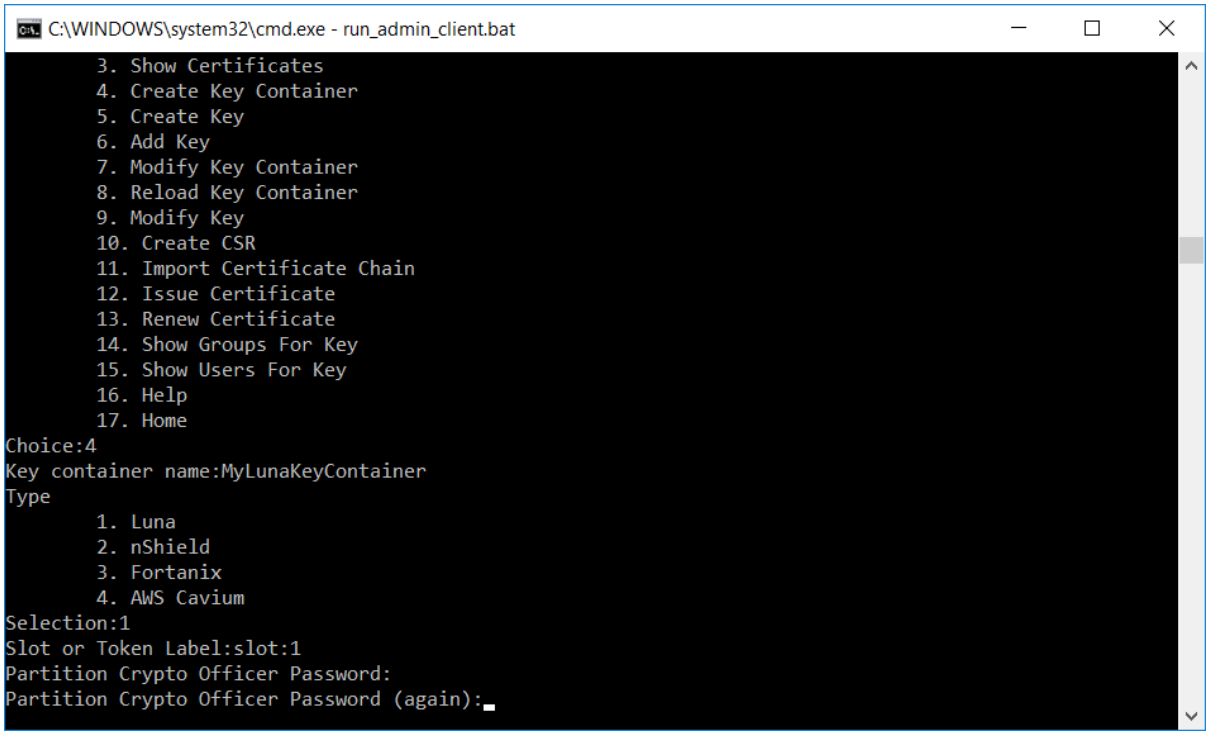


4. Enter the *Slot of Token Label*. If entering the slot value type *slot:<your slot number>* and then press enter. If entering the token label type *tokenlabel:<your token label>* and then press enter.
   Slot example: *slot:1*

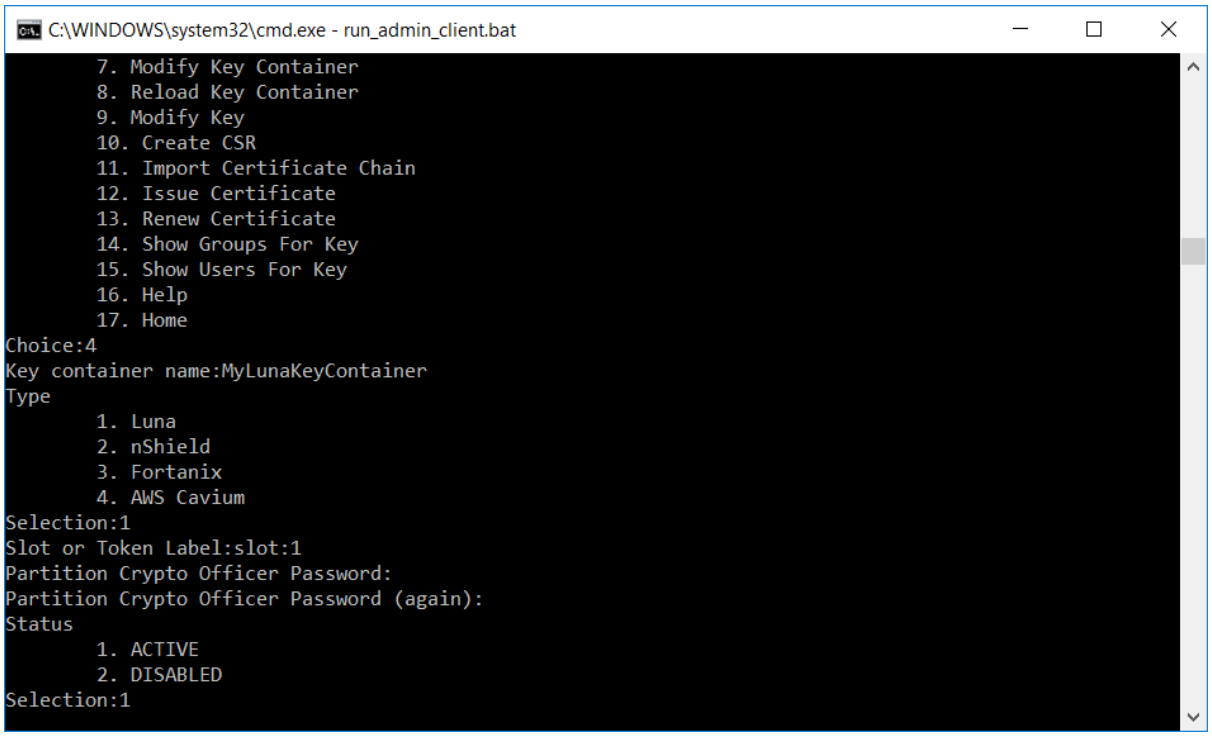
Token Label example: *tokenlabel:mytokenlabel*



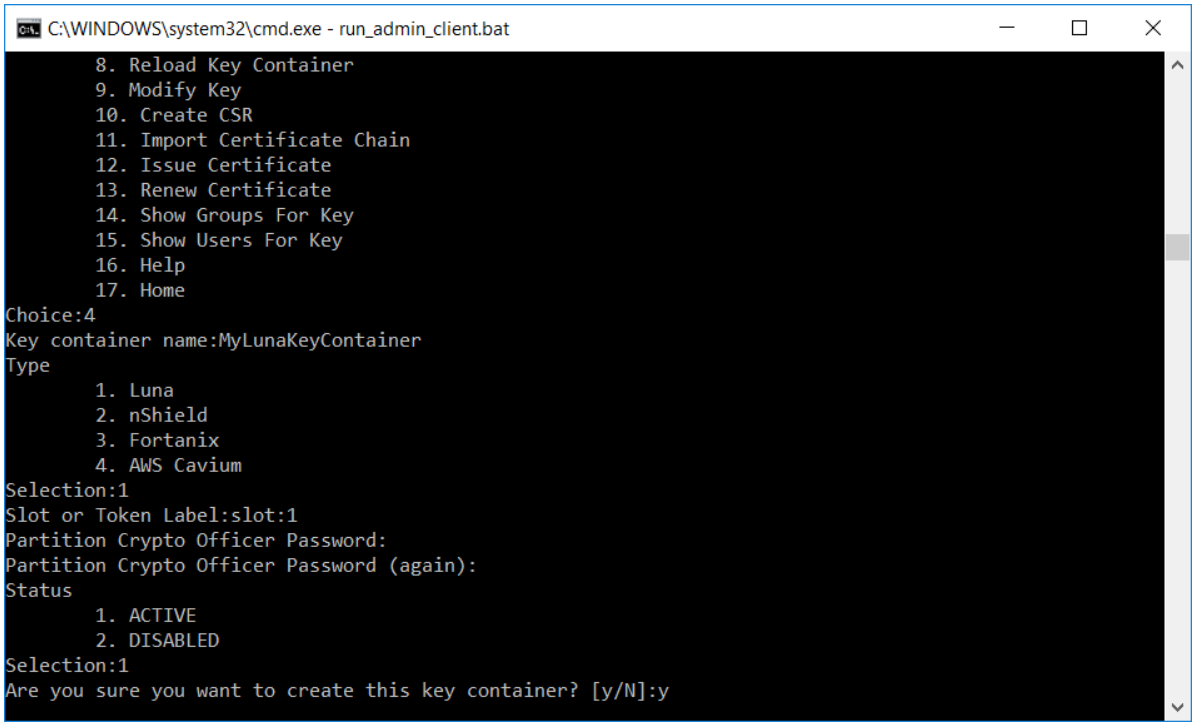
5. Enter the *Crypto Officer Password*. You will be prompted for this twice.



6. 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.



7. 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.



8. Once confirmed, the process may take several moments to connect to your Luna HSM cluster. Please be patient.

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 the Luna HSM?

GaraSign makes use of the native Luna client and software, including the Luna's HA capabilities. Please see your Luna documentation for more information.

Does using the Luna HSM 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.

Is it possible to place GaraSign in the cloud but still use a Luna HSM?

GaraSign is designed to run on-premise, in the cloud, or in a hybrid environment. For customers who wish to keep their Luna HSMs on-premise but utilize the cloud for scaling, GaraSign servers in the cloud can make use of the on-premise HSMs provided that network connectivity is available. Customers can also choose to connect their GaraSign instance to an HSM in the cloud using SafeNet Data Protection on Demand.

How can I integrate GaraSign with SafeNet Data Protection on Demand (DPoD)?

After registering your DPoD account, launch an HSM on Demand (HSMoD). Once your HSMoD service partition is configured, follow the Luna HSM Integration steps above to integrate your HSMoD with GaraSign.

Where can I find more information on setting up my DPoD environment?

Please see the following links:

- DPoD account registration
- Adding a HSMoD Service
- Configuring the HSMoD Service Partition