GaraSign Fortanix DSM Integration

Table of Contents

Preface 2

Document Information 2

Trademarks 2

Disclaimer 2

Document Overview 2

Intended Audience 2

GaraSign Overview 3

Fortanix DSM Integration 4

Create Fortanix Key Container 4

Frequently Asked Questions 5

Are the keys exportable to the client? 5

How is High Availability (HA) achieved with the Fortanix DSM? 5

Does using the Fortanix DSM slow down the process of signing? 5

Is it possible to place GaraSign in the cloud but still use a Fortanix DSM? 5

Preface

Document Information

Title	GaraSign Fortanix DSM 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 Fortanix DSM as its key container. The Fortanix DSM may be used on-premise or hosted in the cloud.

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 Fortanix DSM

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.

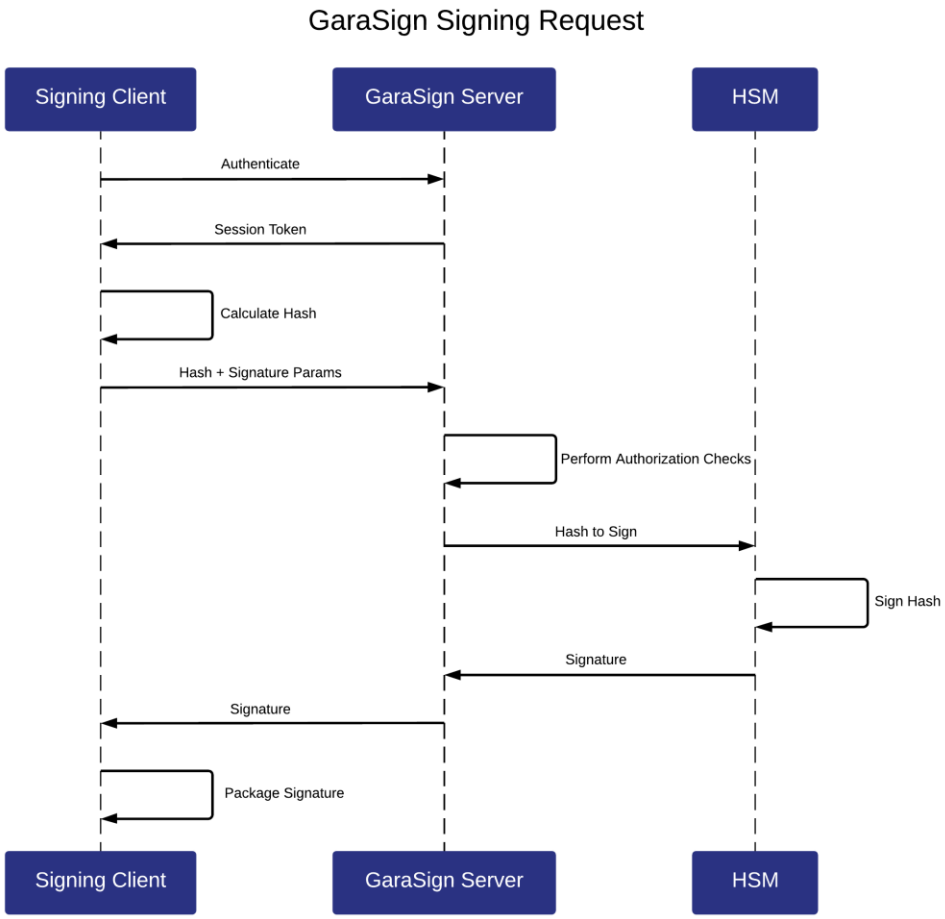

Figure 1 - GaraSign Signing Request

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.

Fortanix DSM Integration

Integrating GaraSign with the Fortanix DSM is done by performing the following steps on each GaraSign Signing and Administration server:

1. Install and configure the Fortanix DSM PKCS#11 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. Start (or restart) the Tomcat instances on the Signing and Administration servers
4. From the GaraSign Administrative Console, create a key container of type Fortanix

Details for step 1 can be found in your Fortanix DSM documentation. Please make sure that the user that Tomcat runs as has read and execute permissions to the Fortanix DSM PKCS#11 library.

Step 2 is handled by your GaraSign professional services personnel.

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

Create Fortanix Key Container

Follow the steps from your GaraSign Admin User Guide documentation to launch the GaraSign Administrative CLI and login. Once logged in, execute the following steps:

1. From the *Main Menu* select *Key Management, Key Container 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 *Fortanix.*
4. Enter the *PKCS#11 Library Path*.
5. Enter the *API Key*. 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.
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 Fortanix DSM. Please be patient. If the process does not complete successfully, please check the server-side logs on the GaraSign administrative servers for more information.

Once complete, the Fortanix DSM can be used like any other key container in GaraSign. You can now use the Fortanix DSM with GaraSign to create keys, generate certificate signing requests (CSRs), import certificates, sign and decrypt data, and more.

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 Fortanix DSM?

GaraSign makes use of the native Fortanix DSM client and software, including its HA capabilities. Please see your Fortanix DSM documentation for more information.

Does using the Fortanix DSM 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 Fortanix DSM?

GaraSign is designed to run on-premise, in the cloud, or in a hybrid environment. For customers who wish to keep their Fortanix DSMs on-premise but utilize the cloud for scaling, GaraSign servers in the cloud can make use of the on-premise DSMs provided that network connectivity is available. Customers can also choose to connect their GaraSign instance to a DSM in the cloud.