GaraSign Utimaco Crypto Server HSM Integration

Table of Contents

Preface 2

Document Information 2

Trademarks 2

Disclaimer 2

Document Overview 2

Intended Audience 2

GaraSign Overview 3

Crypto Server HSM Integration 4

Create Crypto Server Key Container 4

Frequently Asked Questions 5

Are the keys exportable to the client? 5

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

Does using the HSM slow down the process of signing? 5

Is it possible to place GaraSign in the cloud but still use an on-premise HSM? 5

Preface

Document Information

Title	GaraSign Utimaco Crypto Server 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 Utimaco Crypto Server HSM as its key container.

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 Utimaco Crypto Server 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.

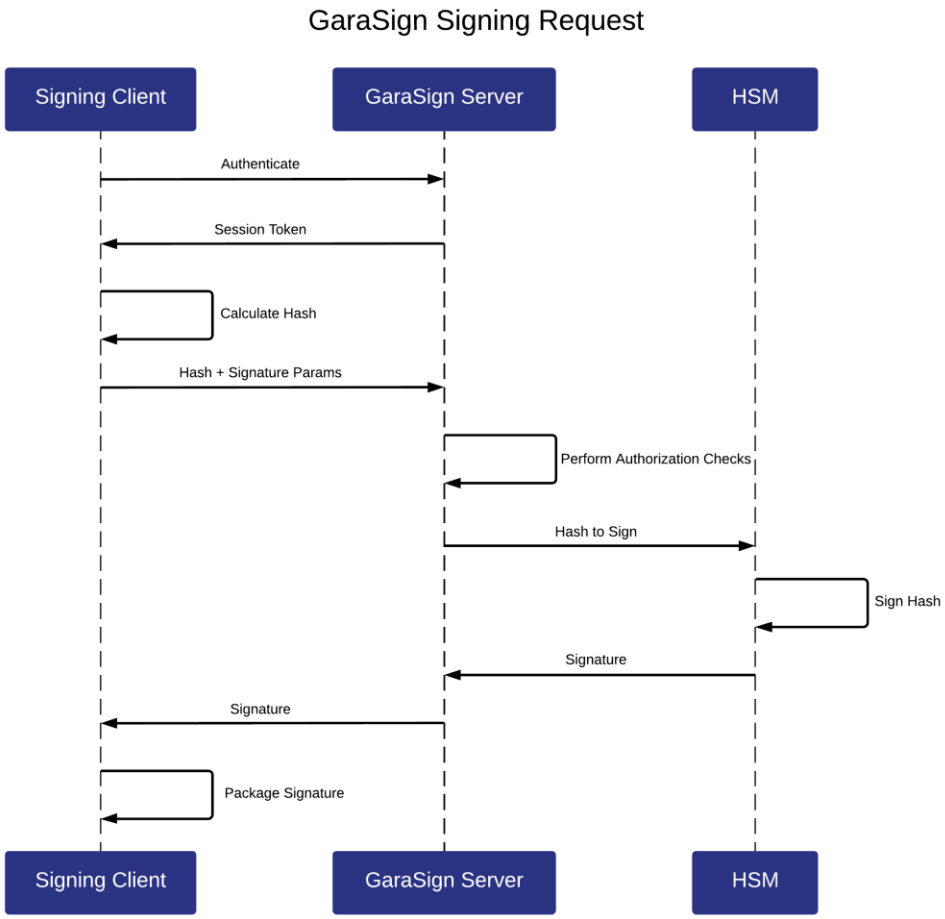

Figure 1 - GaraSign Signing Request

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.

Crypto Server HSM Integration

Integrating GaraSign with the Crypto Server HSM is done by performing the following steps on each GaraSign Signing and Administration server:

1. Install and configure the Crypto Server Client including the 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. Ensure the PKCS#11 provider is in the system path
4. Start (or restart) the Tomcat instances on the Signing and Administration servers
5. From the GaraSign Administrative Console, create a key container of type Utimaco Security Server

Details for step 1 can be found in your Utimaco documentation. Details for step 2 can be found in your GaraSign documentation, although this is typically handled by your GaraSign professional services personnel.

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

Create Crypto Server Key Container

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

1. Under Key Management click on Key Containers.
2. Click the + button to Create a Key Container.
3. For *Key Container Type* choose the *UTIMACO_SECURITY_SERVER.*
4. Provide a Name.
5. If required, set the Slot.
6. Provide the PIN.
7. Click Submit
8. Once confirmed, the process may take several moments to connect to your HSM cluster. Please be patient.

Once complete, the HSM can be used like any other key container in GaraSign. You can now use the HSM 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 HSM?

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

Does using the 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 an on-premise HSM?

GaraSign is designed to run on-premise, in the cloud, or in a hybrid environment. For customers who wish to keep their 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 if they have access to such an HSM.

-