GaraSign nShield HSM Integration

Table of Contents

Preface 2
Document Information 2
Trademarks 2
Disclaimer 2
Document Overview 2
Intended Audience 2
GaraSign Overview 3
Supported Configurations 4
Supported Keys and Algorithms 4
nShield HSM Integration 5
Configure cknfastrc 5
Static Environment 5
Dynamic Environment 5
Create nShield Key Container 5
Frequently Asked Questions 8
Are the keys exportable to the client? 8
How is High Availability (HA) achieved with the nShield HSM? 8
Does using the nShield HSM slow down the process of signing? 8
How fast can GaraSign produce signatures? 8
Is it possible to place GaraSign in the cloud but still use a nShield HSM? 8
Can I use my own Certificate Authority (CA) with GaraSign? 8
Does GaraSign support more than just signing? 8
Where can I learn more? 8

Preface

Document Information

Title	GaraSign nShield HSM Integration
Product Name	GaraSign
Product Version	1.0.0 & above

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 key managers and can even do so simultaneously. This document describes how to integrate GaraSign with the nShield HSM as its key container. The nShield HSM may be used on-premise or hosted in the cloud using nCipher's nShield as a Service.

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 nShield 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 many 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 Signing 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 performed.

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 significantly reduces the integration complexities that your clients must deal with and helps to shield your cryptographic keys from attack and misuse.

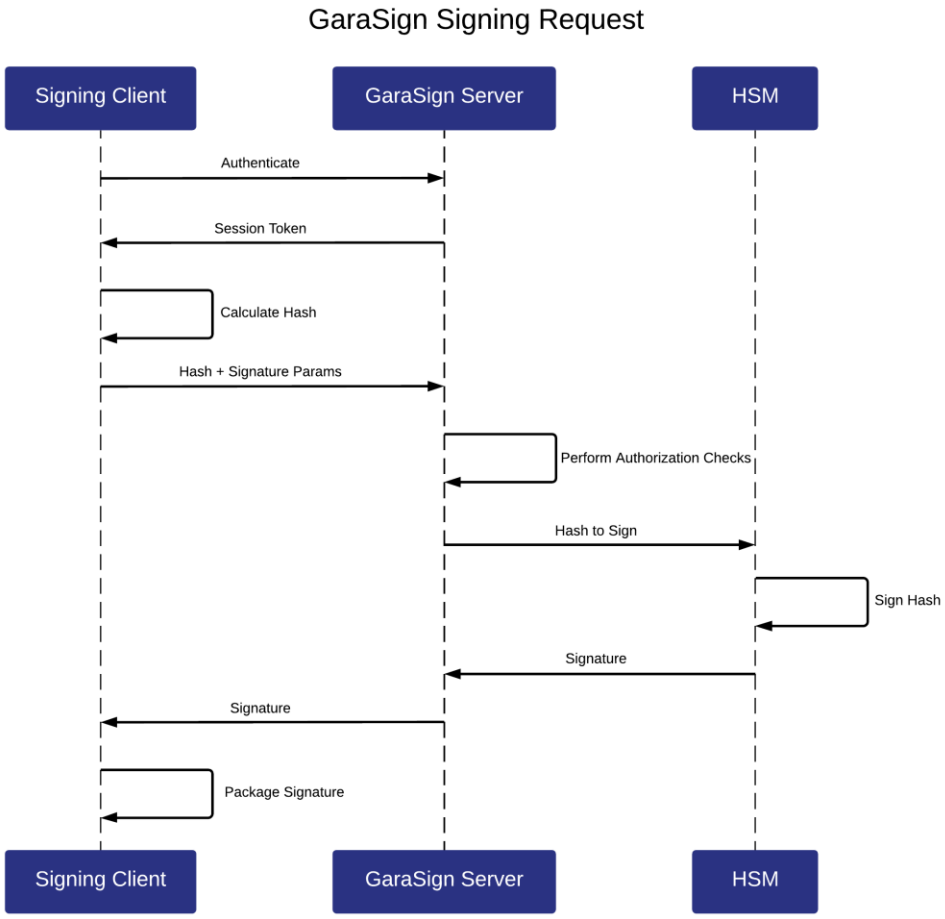

Figure 1 - GaraSign Signing Request

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.

Supported Configurations

All nodes in GaraSign are horizontally scalable and every standard deployment has a minimum of one Signing Server and one Administrative Server. Since the Signing and Administration servers must be on different machines and both must be connected to the HSM, GaraSign integrates with the following network-based nShield HSMs:

Model	Version
Connect XC	12.60
Connect+	V11+

Note: it is possible to deploy a static GaraSign environment where the contents of the HSM will not change after the initial deployment. In this scenario GaraSign can use the nShield Solo as its key container. This deployment model is rarely needed and is out of scope for this document. Please contact your Garantir representative if you wish to learn more about this use case.

Supported Keys and Algorithms

GaraSign supports signing data with module-protected RSA and Elliptic Curve keys (note: the nShield HSM requires the ECC Activation License to use Elliptic Curve keys). While GaraSign does not impose any restrictions on the key size or curve type, the following table provides the list of keys that are officially supported and tested with each GaraSign release:

Key Type	Size/Curve
RSA	2048, 3072, 4096
Elliptic Curve	NIST P-256, NIST P-384, NIST P-521

Clients can sign data using any of the key types listed above with any of the following hash algorithms:

- MD5
- SHA-1
- SHA-224 (SHA-2)
- SHA-256 (SHA-2)
- SHA-384 (SHA-2)
- SHA-512 (SHA-2)
- SHA3-224
- SHA3-256
- SHA3-384
- SHA3-512

nShield HSM Integration

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

1. Install and configure the nShield Client including the Java (JSP) provider
2. Configure the cknfastrc file
3. Install the appropriate GaraSign software for the server type (i.e., GaraSign signing software for Signing Server and GaraSign admin software for Administration Server)
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 nShield

Details for step 1 can be found in your nShield HSM documentation.

Details for step 3 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 steps 2 and 4.

Configure cknfastrc

There are multiple cknfastrc configurations that GaraSign supports but Garantir only recommends two. The appropriate configuration to use depends on whether you have a static or dynamic environment.

Static Environment

A static environment is one where the keys do not change or do so very rarely in a controlled manner. This may be the case when using GaraSign purely for code signing, document signing, and/or certificate issuance. In these environments the recommended cknfastrc configuration is:

```
CKNFAST_FAKE_ACCELERATOR_LOGIN=1

CKNFAST_OVERRIDE_SECURITY_ASSURANCES=none
```

Dynamic Environment

A dynamic environment is one where the keys change often. This may be the case when using GaraSign for S/MIME, TLS, VPN, Zero-Trust, or SSH. In these environments the recommended cknfastrc configuration is:

```
CKNFAST_FAKE_ACCELERATOR_LOGIN=1

CKNFAST_OVERRIDE_SECURITY_ASSURANCES=none

CKNFAST_ASSUME_SINGLE_PROCESS=0
```

Create nShield Key Container

Follow the steps in your GaraSign Admin User Guide documentation to launch the GaraSign Administrative Console 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 the *nShield.*

4. Optionally, choose whether you want to explicitly set the slot.

5. Enter the path to the PKCS#11 library. Note: always use Unix-style slashes, even when working on Windows.

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

```
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:nShieldKeyContainer
Type
        1. Luna
        2. nShield
        3. Fortanix
        4. AWS Cavium
        5. HSM Wrap
Selection:2
Set Slot? [y/N]:N
PKCS#11 Library Path:C:/Program Files/nCipher/nfast/toolkits/pkcs11/cknfast.dll
Set Cardset Passphrase? [y/N]:N
Status
        1. ACTIVE
        2. DISABLED
Selection:1
Are you sure you want to create this key container? [y/N]:y
```

Figure 2 - Key Container Setup

Once complete, the nShield HSM can be used like any other key container in GaraSign. You can now use the nShield HSM with GaraSign to create keys, generate certificate signing requests (CSRs), import certificates, sign and decrypt data, and more. Additionally, further administration of your key container can be done from the more user-friendly web UI, as shown below. For more information on how to use GaraSign for key management, please see your GaraSign Administrative User Guide.

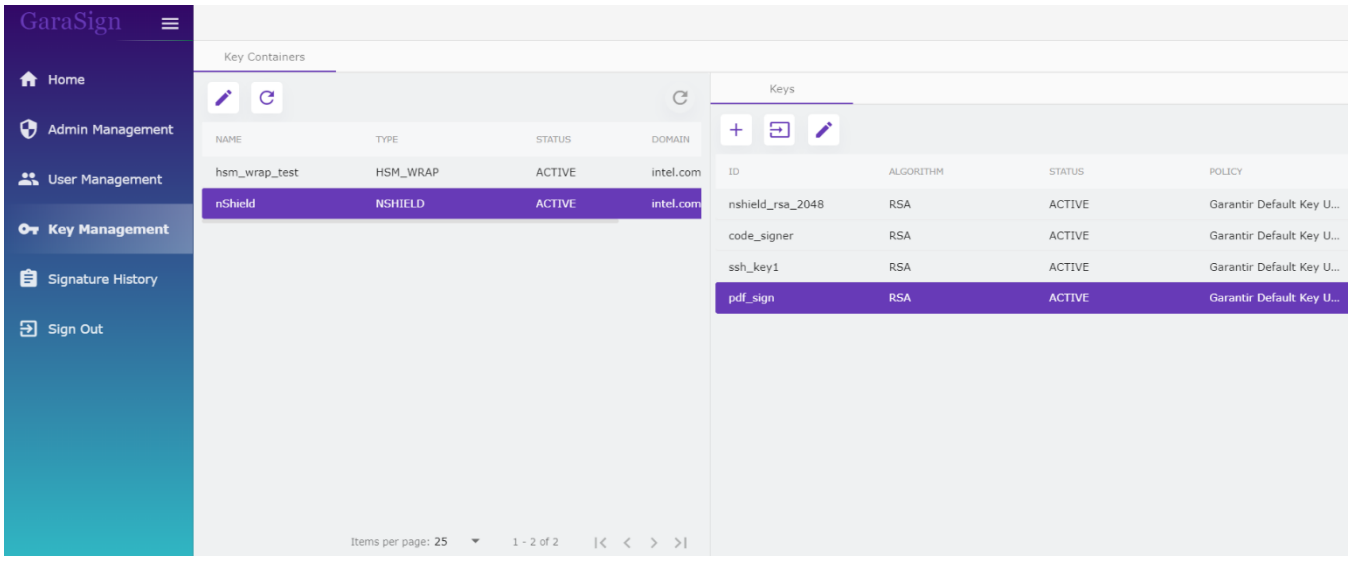

Figure 3 - Menu Expanded

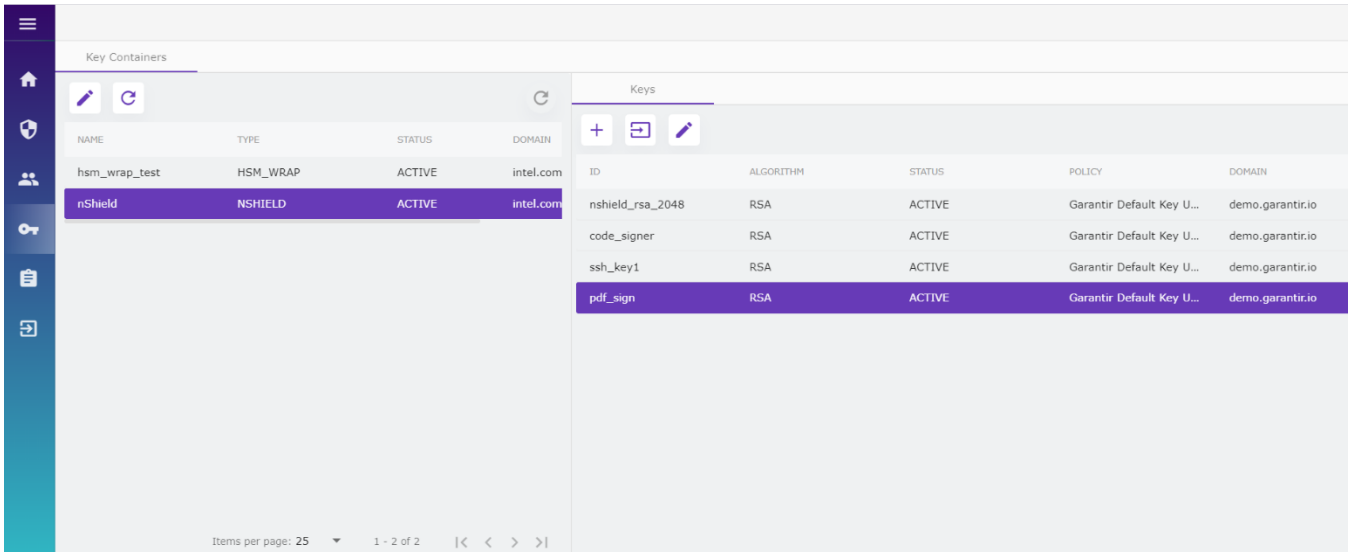

Figure 4 - Menu Collapsed

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 nShield HSM?

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

Does using the nShield 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.

How fast can GaraSign produce signatures?

Extremely fast. The exact speed will be dependent on your environment (e.g., network latency, computer speeds, etc.) but GaraSign's client-side hashing architecture always results in high performance.

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

GaraSign is designed to run on-premise, in the cloud, or in a hybrid environment. For customers who wish to keep their nShield 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 nCipher's nShield as a Service.

Can I use my own Certificate Authority (CA) with GaraSign?

Yes. GaraSign supports multiple CAs and certificate protocols to allow for easy and flexible issuance of certificates. A single GaraSign deployment can integrate with multiple CAs simultaneously allowing for maximum flexibility.

Does GaraSign support more than just signing?

Yes. GaraSign also supports Elliptic-Curve Diffie-Hellman (ECDH) and RSA decryption. In all cases, the private keys are never exported to the client.

Where can I learn more?

Please get in touch with us via email at info@garantir.io.