gemalto
security to be free

PingFederate

INTEGRATION GUIDE

Document Information

Document Part Number	007-000345-001
Release Date	February 2019

Revision History

Revision	Date	Reason
A	February 2019	First Release

Trademarks, Copyrights, and Third-Party Software

Disclaimer

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

PREFACE

This document is intended to guide administrators through the steps for integrating PingFederate with a SafeNet Luna HSM or HSM on Demand Service. This guide provides the necessary information to configure PingFederate to secure the PingFederate SSL certificate and SSO signing keys using a SafeNet Luna HSM or HSM on Demand Service.

Scope

This guide demonstrates configuring a PingFederate test environment that secures the application private keys within a SafeNet Luna HSM or HSM on Demand Service.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

> **NOTE:** Take note. Notes contain important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

> **CAUTION!** Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

> ****WARNING** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury**

Command Syntax and Typeface Conventions

Convention	Description
bold	The bold attribute is used to indicate the following: > Command-line commands and options (Type **dir /p**.) > Button names (Click **Save As**.) > Check box and radio button names (Select the **Print Duplex** check box.) > Window titles (On the **Protect Document** window, click **Yes**.) > Field names (**User Name:** Enter the name of the user.) > Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) > User input (In the **Date** box, type **April 1**.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
Double quote marks	Double quote marks enclose references to other sections within the document.
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>]	Square brackets enclose optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
[a | b | c] [<a> | <b> | <c>]	Square brackets enclose optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

{ a | b | c }
{ <a> | <b> | <c> }
	Braces enclose required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support.

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Gemalto Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support@gemalto.com.

CHAPTER 1: Introduction

PingFederate enables outbound and inbound solutions for single sign-on (SSO), federated identity management, customer identity and access management, mobile identity security, API security, and social identity integration. Browser-based SSO extends employee, customer and partner identities across domains without passwords, using only standard identity protocols (Security Assertion Markup Language—SAML, WS-Federation, WS-Trust, OAuth and OpenID Connect, and SCIM). PingFederate uses the SafeNet Luna HSM or HSMoD service to generate and secure the SSL keys/certificates and signing keys/certificates.

The SafeNet Luna HSM or HSMoD service is an external hardware security module that is available for use with PingFederate. You can use the SafeNet solution with PingFederate to secure RSA and ECDSA Private keys used for signing and SSL. If using a SafeNet Luna HSM you can integrate multiple HSMs as a High Availability (HA) group with PingFederate.

The benefits of using a SafeNet Luna HSM or HSMoD service to generate the Private keys used for SSL & Signing in PingFederate include:

- Secure generation, storage and protection of the private keys on FIPS 140-2 level 3 validated hardware.*
- Full life cycle management of the keys.
- HSM audit trail.**
- Significant performance improvements by off-loading cryptographic operations from servers.

*validation for HSMoD services in progress.
**HSMoD services do not have access to the secure audit trail.

Third Party Application Details

This integration uses the following third party applications:

- PingFederate

  You can download PingFederate from the Ping Identity support site:
  https://support.pingidentity.com/s/product-help-home

Supported Platforms

List of the platforms which are tested with the following HSMs:

SafeNet Luna HSM: SafeNet Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. SafeNet Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing.

The SafeNet Luna HSM on premise offerings include the SafeNet Luna Network HSM, SafeNet PCIe HSM, and SafeNet Luna USB HSMs. SafeNet Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic

The following platforms are supported:

Platforms Tested	PingFederate	SafeNet HSM
RHEL 7.6 (64 bit) Windows Server 2016 Standard	PingFederate v9.2	SafeNet Luna SA 6.3.0 Firmware 6.27.0 SafeNet Luna Client 6.3.0
RHEL 7.6 (64 bit) Windows Server 2016 Standard	PingFederate v9.2	SafeNet Luna SA 7.2.0 Firmware 7.2.0 SafeNet Luna Client 7.2.0

NOTE: PingFederate is supported with Luna Clients in HA & FIPS Mode.

SafeNet DPoD: SafeNet Data Protection on Demand (DPoD) is a cloud-based platform that provides on-demand HSM and Key Management services through a simple graphical user interface. With DPoD, security is simple, cost effective and easy to manage because there is no hardware to buy, deploy and maintain. As an Application Owner, you click and deploy services, generate usage reports and maintain just the services you need.

The following platforms are supported:

Platforms Tested	PingFederate	SafeNet HSM
RHEL 7.6 (64 bit) Windows Server 2016 Standard	PingFederate v9.2	SafeNet HSM on Demand v1.7

Prerequisites

Before you proceed with the integration, complete the following:

Configure SafeNet Luna HSM

If you are using a SafeNet Luna HSM, ensure the following:

1. Ensure the HSM is set up, initialized, provisioned and ready for deployment. Refer to the SafeNet Luna HSM Product Documentation for more information.
2. Create a partition on the SafeNet Luna HSM for use with PingFederate.
3. If using a SafeNet Luna Network HSM, register a client for the system and assign the client to each partition to create an NTLS connection for the three partitions. Initialize the Crypto Officer and Crypto User roles for each registered partition.
4. Ensure that each partition is successfully registered and configured. The command to see the registered partitions is:

```
# /usr/safenet/lunaclient/bin/lunacm
  LunaCM v7.2.0. Copyright (c) 2006-2017 SafeNet.
Available HSMs:
   Slot Id ->               0
   Label ->                 pingfed
   Serial Number ->         1238712343066
   Model ->                 LunaSA 7.2.0
   Firmware Version ->      7.2.0
   Configuration ->         Luna User Partition With SO (PED) Key Export With
Cloning Mode
   Slot Description ->      Net Token Slot
```

> **NOTE:** Follow the *SafeNet Luna Network HSM Product Documentation* for detailed steps for creating the NTLS connection, initializing the partitions, and initializing the Security Officer, Crypto Officer, and Crypto User roles.

Provision your HSM on Demand Service

This service provides your client machine with access to an HSM Application Partition for storing cryptographic objects used by your applications. Application partitions can be assigned to a single client, or multiple clients can be assigned to, and share, a single application partition.

To use the HSM on Demand service you need to provision your application partition, starting by initializing the following roles:

- **Security Officer (SO)** - responsible for setting the partition policies and for creating the Crypto Officer.
- **Crypto Officer (CO)** - responsible for creating, modifying and deleting crypto objects within the partition. The CO can use the crypto objects and create an optional, limited-capability role called Crypto User that can use the crypto objects but cannot modify them.
- **Crypto User (CU)** - optional role that can use crypto objects while performing cryptographic operations.

> **NOTE:** Refer to the SafeNet Data Protection on Demand Application Owner Quick Start Guide for procedural information on configuring the HSM on Demand service and create a service client.
>
> The HSM on Demand service client package is a zip file that contains system information needed to connect your client machine to an existing HSM on Demand service

Constraints on SafeNet HSMs

Please take the following limitations into consideration when provisioning your HSMoD services:

SafeNet Luna HSM or HSM on Demand Services in FIPS Mode

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using the SafeNet Luna HSM or an HSMoD service in FIPS mode, you have to make the following change in configuration file:

```
Misc = {
   RSAKeyGenMechRemap = 1;
}
```

The above setting redirects the older calling mechanism to a new approved mechanism when SafeNet Luna HSM or the HSMoD service is in FIPS mode.

> **NOTE:** The above configuration is valid for Luna HSM f/w v6.22.0 and above only. Execute “hsm firmware show” in lunash to verify the firmware version.

HSM on Demand Service in FIPS mode

HSMoD services operate in a FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, ensure you enable the **Allow non-FIPS approved algorithms** check box when configuring your HSM on Demand service. The FIPS mode is enabled by default.

Refer to the *Mechanism List* in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.

Verify HSM on Demand <slot> value

LunaCM commands work on the current slot. If there is only one slot, then it is always the current slot. If you are completing an integration using HSMoD services, you need to verify which slot on the HSMoD service you send the commands to. If there is more than one slot, then use the **slot set** command to direct a command to a specified slot. You can use **slot list** to determine which slot numbers are in use by which HSMoD service.

Controlling User Access to the HSM

For Luna Client 7.x onwards, by default, only the root user has access to the HSM. You can specify a set of non-root users that are permitted to access the HSM by adding them to the **hsmusers** group. The client software installation automatically creates the **hsmusers** group. The **hsmusers** group is retained when you uninstall the client software, allowing you to upgrade your client software while retaining your **hsmusers** group configuration.

To allow non-root users or applications access to the HSM, assign the users to the **hsmusers** group.

> **NOTE:** The users you assign to the **hsmusers** group must exist on the client workstation.

> **Adding user to hsmusers group**

a. Ensure that you have **sudo** privileges on the client workstation.

b. Add a user to the hsmusers group.

```
sudo gpasswd --add <username> hsmusers
```

Where `<username>` is the name of the user you want to add to the hsmusers group.

To revoke a user's access to the HSM, you can remove them from the hsmusers group.

> **Removing a user from hsmusers group**

a. Ensure that you have **sudo** privileges on the client workstation.

b. Remove a user from the hsmusers group.

```
sudo gpasswd -d <username> hsmusers
```

Where `<username>` is the name of the user you want to remove from the hsmusers group. You must log in again to see the change.

> **NOTE:** The user you delete will continue to have access to the HSM until you reboot the client workstation.

Set up PingFederate

PingFederate server is based on J2EE application server technology. The product documentation for PingFederate are available at the following link under **Documentation.** https://support.pingidentity.com/s/PingFederate-help

CHAPTER 2: Integrating PingFederate with SafeNet HSM

SafeNet Luna HSM or HSMoD Service integrates with PingFederate to secure the SSL certificate and SSO signing keys.

Before you begin

Before using SafeNet Luna HSM or HSMoD service with the PingFederate, you must ensure that:

- The SafeNet HSM appliance or HSMoD service and the PingFederate server can communicate with each other.
- The SafeNet HSM appliance has a virtual HSM (HSM Partition) defined before you install the client software on the PingFederate.
- The SafeNet Luna Client or HSMoD Client is installed on your network, including the package for Java (referred to as the JSP).

Configuring the SafeNet Luna HSM or HSMoD Client for PingFederate

Edit the PingFederate configuration files to use the SafeNet Luna Provider Library and then sign in to the HSM through PingFederate.

To configure the SafeNet Luna HSM or HSMoD client for PingFederat

1. Set the **JAVA_HOME** environment variable to the Java installation directory path and add its bin directory to the PATH environment variable.

   For Linux:

   ```
   # export JAVA_HOME=<installed JRE path>
   # export PATH=$JAVA_HOME/bin:$PATH
   ```

   For Windows:
   Set the **JAVA_HOME** variable and modify **PATH** variable at the system level

2. Configure Java to use SafeNet Luna Provider, copy the Luna library and Luna Provider jar to the Java installation as follows:

Operating system	Steps
Windows	Copy the **<Luna installation directory>\jsp\lib\LunaAPI.dll** file to an arbitrary directory and add the directory's path as a system variable. Alternatively, you can copy the file to the Windows system directory (**C:\Windows\System32**).

Operating system	Steps
	Copy the **<Luna installation directory>\jsp\lib\LunaProvider.jar** file to the **JAVA_HOME\jre\lib\ext** directory. **LunaProvider.jar** and **libLunaAPI.so** for HSMoD are available at below location: **<DPoD client directory>/LunaProvider.jar** **<DPoD client directory>/libLunaAPI.so**
Linux	Copy the **libLunaAPI.so** and **LunaProvider.jar** files from the **<Luna installation directory>/jsp/lib** directory to the **JAVA_HOME/jre/lib/ext** directory. **LunaProvider.jar** and **libLunaAPI.so** for HSMoD are available at below location: **<DPoD client directory>/jsp/LunaProvider.jar** **<DPoD client directory>/jsp/64/libLunaAPI.so**

3. Edit the **JAVA_HOME/jre/lib/security/java.security** file in your Java environment and add the LunaProvider line to the list of security providers, immediately before the **sun.security.ec.SunEC** provider line:

```
security.provider.1=sun.security.provider.Sun

security.provider.2=sun.security.rsa.SunRsaSign

security.provider.3=com.safenetinc.luna.provider.LunaProvider

security.provider.4=sun.security.ec.SunEC

security.provider.5=com.sun.net.ssl.internal.ssl.Provider

security.provider.6=com.sun.crypto.provider.SunJCE

security.provider.7=sun.security.jgss.SunProvider

security.provider.8=com.sun.security.sasl.Provider

security.provider.9=org.jcp.xml.dsig.internal.dom.XMLDSigRI

security.provider.10=sun.security.smartcardio.SunPCSC
```

4. Edit the **hivemodule.xml** file in the **<pf_install>/pingfederate/server/default/conf/META-INF** directory and update the **<!-- Crypto provider -->** section.

   - For the **JCEManager** service endpoint, change the value of the construct class to as follows:

     ```
     <construct class="com.pingidentity.crypto.LunaJCEManager6"/>
     ```

   - For the **CertificateService** service endpoint, change the value of the construct class as follows:

     ```
     <construct class="com.pingidentity.crypto.LunaCertificateServiceImpl6"/>
     ```

5. Edit the **<pf_install>/pingfederate/bin/run.properties** file.

   a. Change the value of the **pf.hsm.mode** property from **OFF** to **LUNA**.

      ```
      pf.hsm.mode=LUNA
      ```

   b. Change the value of the **pf.hsm.mode** property to **true**

```
pf.hsm.hybrid=true
```

If you are setting up a new PingFederate installation, set the value of the **pf.hsm.hybrid** property to **false**. When set to false, as you create or import certificates (such as your signing certificate or your encryption key), the certificates are stored on your HSM.

If you are configuring an existing PingFederate installation, set the **pf.hsm.hybrid** to **true**, which provides the flexibility to store each relevant key and certificate on the HSM or the local trust store. This capability allows you to transition the storage of keys and certificates to your HSM without the need to deploy a new PingFederate environment and to mirror the setup.

6. From the **<pf_install>/pingfederate/bin** directory, run the **hsmpass.bat** batch file for Windows or the **hsmpass.sh** script for Linux. Enter the NTLS password when prompted.

   This procedure sets and securely stores the password for NTLS communication to the HSM from PingFederate.

7. Edit the **com.pingidentity.crypto.LunaPartitions.xml file** in the **<pf_install>/pingfederate/server/default/data/config-store** directory and update the **<con:config>** section.

   For the **con:item,** change the value of **name** to as follows:

   ```
   <con:item name="DefaultPartitionSlotOrLabel">tokenlabel:label</con:item>
   ```

   Where label is the HSM partition name.

8. If using an HSMoD service, create the soft link which point to the HSMoD configuration file in /etc directory.

   ```
   # ln -sf <DPoD client directory>/Chrystoki.conf /etc/Chrystoki.conf
   ```

   This completes the steps required to configure PingFederate for use with the SafeNet HSMs. You are required start or restart the PingFederate server for changes to take effect.

Managing Keys and Certificate on SafeNet HSMs

Generate keys and certificates on the SafeNet HSMs through the PingFederate Administrative console. This integration guide contains procedures for the following:

> Managing SSL Server Certificates

> Managing SSL Client Keys & Certificates

> Managing Digital Signing Certificates and Decryption Keys

Managing SSL Server Certificates

Use the **Security** > **SSL Server Certificates** screen to establish and maintain the certificates presented for access to the PingFederate administrative console and for incoming HTTPS connections at runtime.

To create a new certificate

1. On the **SSL Server Certificates** screen, click **Create new**.
2. On the **Create Certificate** screen, enter the required information.

For information about each field, refer to the following table:

Field	Description
Common Name	The common name (CN) identifying the certificate.
Subject Alternative Names	The additional DNS names or IP addresses that can be associated with the certificate.
Organization	The organization (O) or company name creating the certificate.
Organizational Unit	The specific unit within the organization (OU).
City	The city or other primary location (L) where the company operates.
State	The state (ST) or other political unit encompassing the location.
Country	The country (C) where the company is based.
Validity (days)	The time during which the certificate is valid.
Cryptographic Provider	The storage facility of the certificate. Select **HSM** to store the certificate in the HSM.
Key Algorithm	A cryptographic formula used to generate a key. PingFederate uses either of two algorithms, RSA or EC.
Key Size (bits)	The number of bits used in the key.
Signature Algorithm	The signing algorithm of the certificate.

3. When finished, click **Next**.
4. Ensure that check boxes **Make this an active certificate for the Runtime Server** and **Make this an active certificate for the Admin Console** are selected. Click **Done**.
5. On the **Summary** screen, review your configuration, amend as needed, and click **Save**.

To create a certificate-authority signing request (CSR)

1. On the **SSL Server Certificates** screen, select **Certificate Signing** under **Action** for the certificate.

   > **NOTE:** This selection is inactive if you have not yet saved a newly created or imported certificate. Click Save and then return to this screen to initiate the process.

2. On the **Certificate Signing** screen, select the **Generate CSR** option.
3. On the **Generate CSR** screen, click **Export** to save the CSR file and click **Done**.
4. Once saved, you can submit this CSR file to a certificate authority (CA) to obtain a CA-signed certificate.

To import a certificate-authority response (CSR response)

1. On the **SSL Server Certificates** screen, select **Certificate Signing** under **Action** for the certificate.
2. On the **Certificate Signing** screen, select the **Import CSR Response** option.
3. On the **Import CSR Response** screen, choose the applicable CSR response file.

4. On the **Summary** screen, review your configuration, click **Save** to keep your configuration or click **Cancel** to discard it.

To import a certificate and its private key

1. On the **SSL Server Certificates** screen, click **Import**.
2. On the **Import Certificate** screen, choose the applicable certificate file and enter its password.
3. Select **HSM** to store the certificate in the HSM.
4. On the **Summary** screen, review your configuration, amend as needed, click **Save** to keep your configuration or click **Cancel** to discard it.

Managing SSL Client Keys & Certificates

On the **Security** > **SSL Client Keys & Certificates** screen, create and manage your authentication private keys and the certificates your server presents as a client in an outbound SSL/TLS transaction. Steps to manage the SSL Client Keys & Certificates on SafeNet HSMs are similar to Manage SSL Server Certificates

Managing Digital Signing Certificates and Decryption Keys

On the **Security** > **Signing & Decryption Keys & Certificates** screen, create and maintain certificates for the purpose of signing outgoing requests, responses, assertions, and access tokens, and for the purpose of decryption. Steps to manage the Digital Signing Certificates and Decryption Keys on SafeNet HSMs are similar to Manage SSL Server Certificates

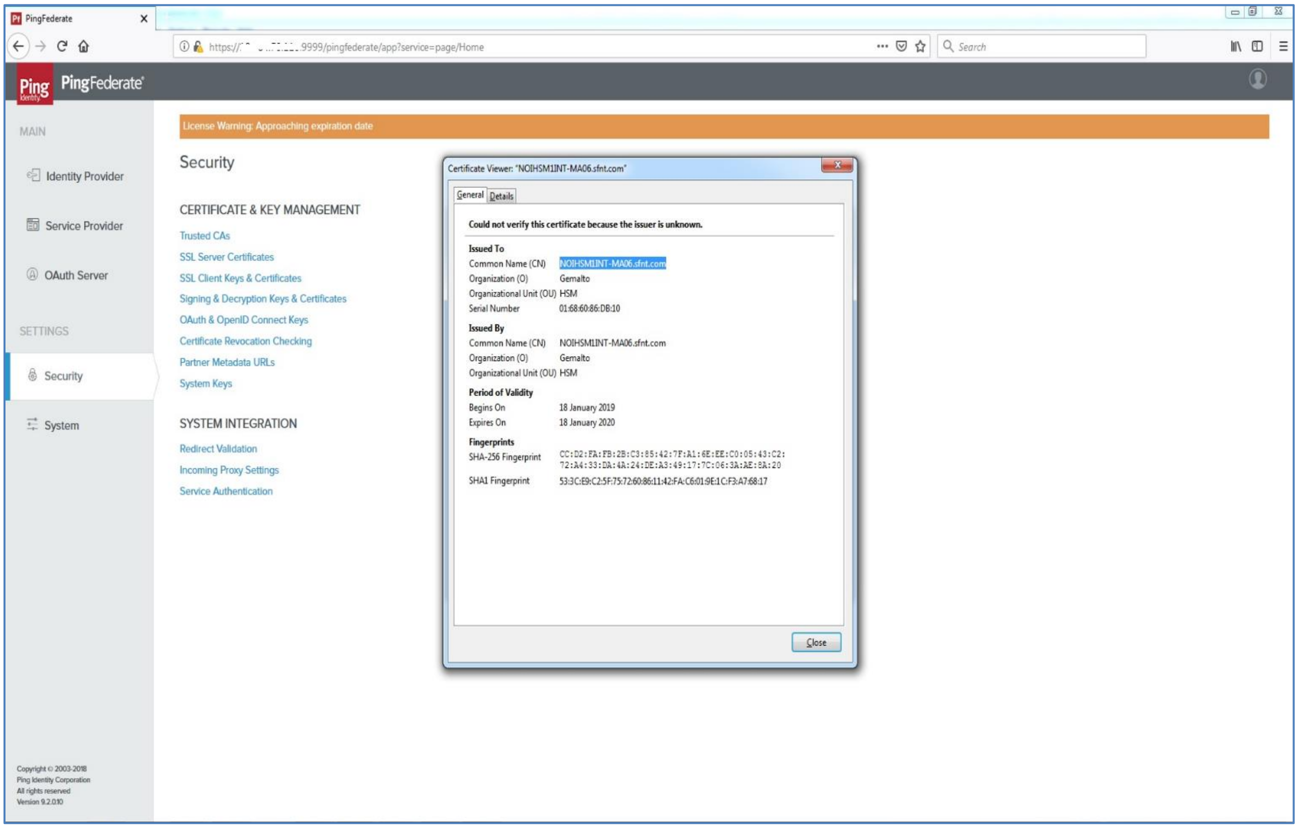
Configuring SSL Server Certificate generated on SafeNet HSMs

Use the **Security** > **SSL Server Certificates** screen to configure the SSL certificate for PingFederate Server.

To configure SSL Server Certificate generated on a SafeNet HSMs

1. On the **SSL Server Certificates** screen, select **Activate Default for Admin Console** under **Action** for the HSM generated certificate.
2. On the **SSL Server Certificates** screen, select **Activate Default for Runtime Server** under **Action** for the HSM generated certificate.
3. Click **Save**.

Open the administrative console and verify that the default certificate is replaced with HSM generated certificate for SSL.



Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	NOIHSM1INT-MA06.sfnt.com
Organization (O)	Gemalto
Organizational Unit (OU)	HSM
Serial Number	01:68:60:86:DB:10

Issued By

Common Name (CN)	NOIHSM1INT-MA06.sfnt.com
Organization (O)	Gemalto
Organizational Unit (OU)	HSM

Period of Validity

Begins On	18 January 2019
Expires On	18 January 2020

Fingerprints

SHA-256 Fingerprint	CC:D2:FA:FB:2B:C3:85:42:7F:A1:6E:EE:C0:05:43:C2: 72:A4:33:DA:4A:24:DE:A3:49:17:7C:06:3A:AE:8A:20
SHA1 Fingerprint	53:3C:E9:C2:5F:75:72:60:86:11:42:FA:C6:01:9E:1C:F3:A7:68:17

Verifying the SSO Feature Provided by Java Integration Kit Using SafeNet HSMs

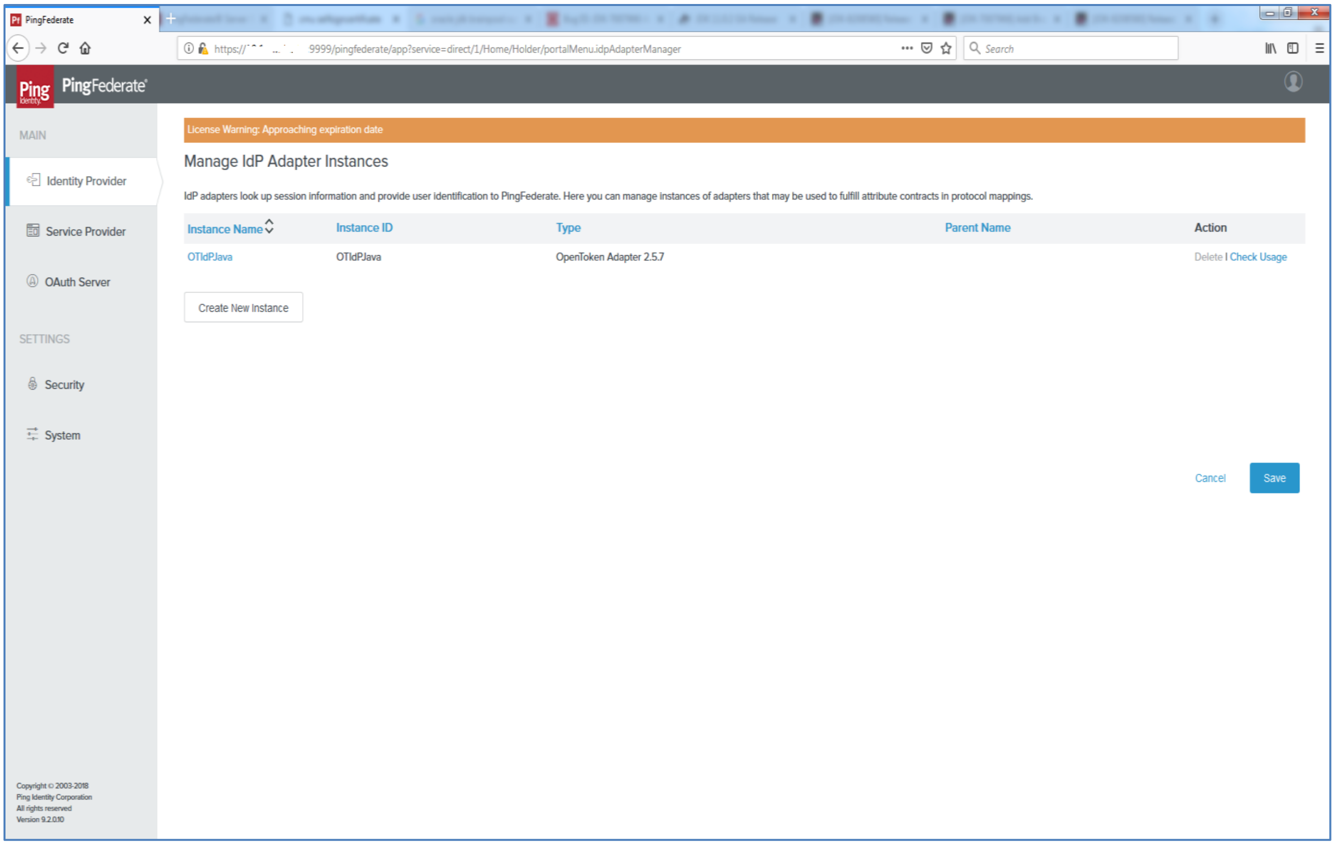
The Java Integration Kit distribution contains sample IdP and SP applications. The applications may be installed quickly for testing OpenToken processing and to provide a working demonstration of end-to-end single sign-on (SSO) and single logout (SLO). The Java Integration Kit can be downloaded from Ping Identity resource download page. https://www.pingidentity.com/en/resources/downloads/pingfederate.html

> **NOTE:** Ensure the Java Integration Kit is installed and configured before configuring the SafeNet Luna or HSMoD Client with PingFederate.
>
> Also Sample Applications provided by Java Integration Kit is using SHA1_HMAC mechanism that is not permitted for signing when HSM in FIPS mode. For running Java Sample Application use HSM in Non-FIPS mode.

1. Follow the Ping Federate Java Integration Kit documentation to install and configure the OpenToken Adapter for both an IdP and an SP as well as deploy the Java agent.

   https://docs.pingidentity.com/bundle/javaIK25_sm_JavaIntegrationKit/page/javaIK_c_JavaIntegrationKit.html

2. After installing, verify your Sample Applications are deployed successfully.



License Warning: Approaching expiration date

Manage IdP Adapter Instances

IdP adapters look up session information and provide user identification to PingFederate. Here you can manage instances of adapters that may be used to fulfill attribute contracts in protocol mappings.

Instance Name	Instance ID	Type	Parent Name	Action
OTIdPJava	OTIdPJava	OpenToken Adapter 2.5.7		Delete I Check Usage

Create New Instance

Now configure the Ping Federate to use HSM by steps provided in Configuring the SafeNet Luna HSM or HSMoD Client for PingFederate and generate the Signing & Decryption Keys & Certificates.

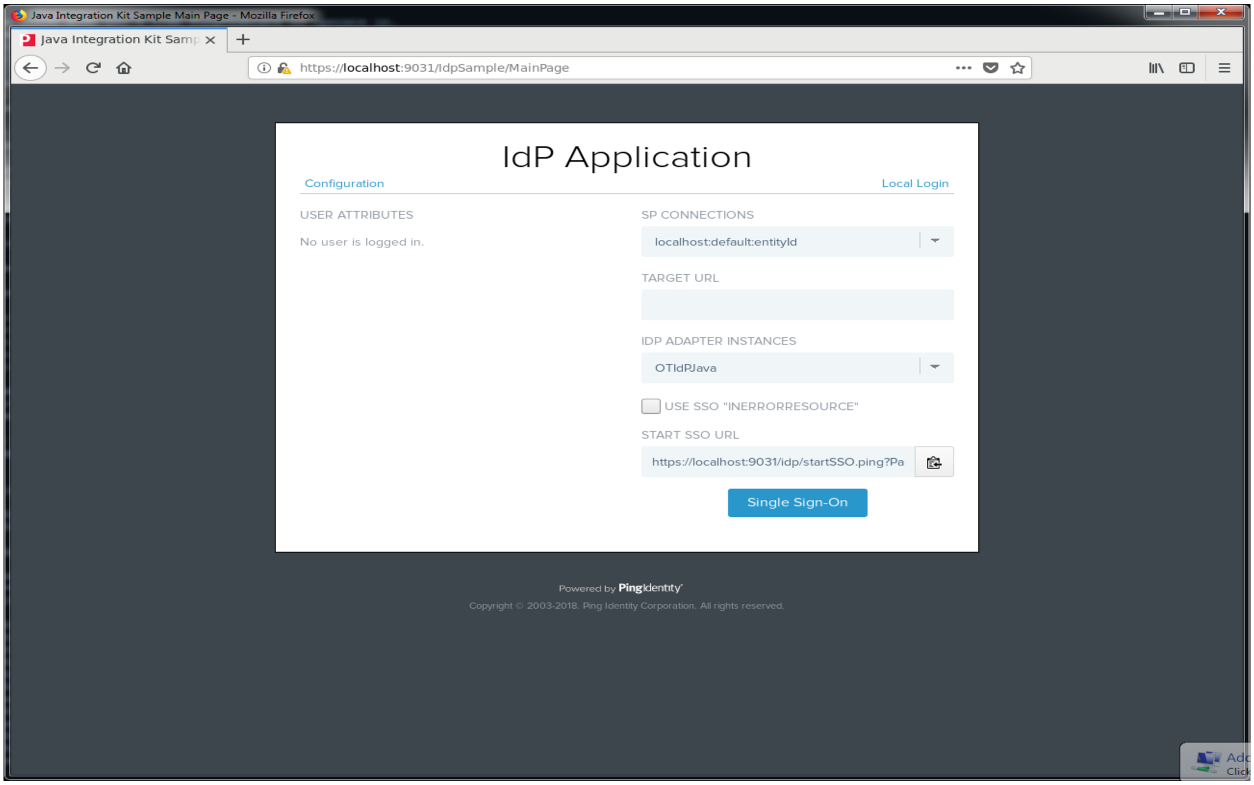
Use the certificate generated on SafeNet HSM as SSO signing certificate for IdP and SP application provided by Ping Federate Java Integration Kit, perform the steps below.

To verify the SSO Feature Provided by Java Integration Kit Using SafeNet HSMs

1. Log in to the PingFederate Administrative Console.
2. Click **Security** > **Signing & Decryption Keys & Certificates**.
3. Under **Action**, click **Export**.
4. Click **Next** and then **Export** to export the certificate.
5. Click **Save File** when prompted and Click **Done**.
6. Click **Identity Provider**.
7. Under **SP Connections** click the **SAML2.0** entity.
8. On SP Connection Page, Click **Credentials** > **Configure Credentials** > **Digital Signature Settings**.
9. Select the **Signing Certificate** generated on the SafeNet HSM and the **Signing Algorithm**. Click **Next**.
10. Click **Manage Signature Verification Settings** > **Signature Verification Certificates** > **Manage Certificates** > **Import**.
11. Import the certificate. Click **Choose File** and select the certificate exported from HSM in step 3. Click **Next**.

12. Ensure that the **Make this an active verification certificate** check box is selected. Click **Done**.
13. Click **Done** to confirm the certificate. Click **Save.**
14. Click **Service Provider**.
15. Under **IdP Connections** click the **SAML2.0** entity.
16. On **IdP Connection** Page, Click **Credentials** > **Configure Credentials** > **Digital Signature Settings**.
17. Select the **Signing Certificate** generated on SafeNet HSM and the **Signing Algorithm**. Click **Next**.
18. Click **Manage Signature Verification Settings** > **Signature Verification Certificates** > **Manage Certificates** > **Import**.
19. To import certificate click **Choose File** and select the certificate exported from HSM in step 3. Click **Next.**
20. Ensure that **Make this an active verification certificate** check box is selected, click **Done**.
21. Click **Done** to confirm the certificate. Click **Save.**
22. Restart the PingFederate service for changes to take effect.
23. Open the browser and access the IdP Sample application URL.

    https://localhost:9031/IdpSample


Java Integration Kit Sample Main Page - Mozilla Firefox
Java Integration Kit Samp
Configuration
Local Login
Single Sign-On
Powered by PingIdentity

https://localhost:9031/IdpSample/MainPage

IdP Application

USER ATTRIBUTES

No user is logged in.

SP CONNECTIONS: localhost:default:entityId

TARGET URL:

IDP ADAPTER INSTANCES: OTIdPJava

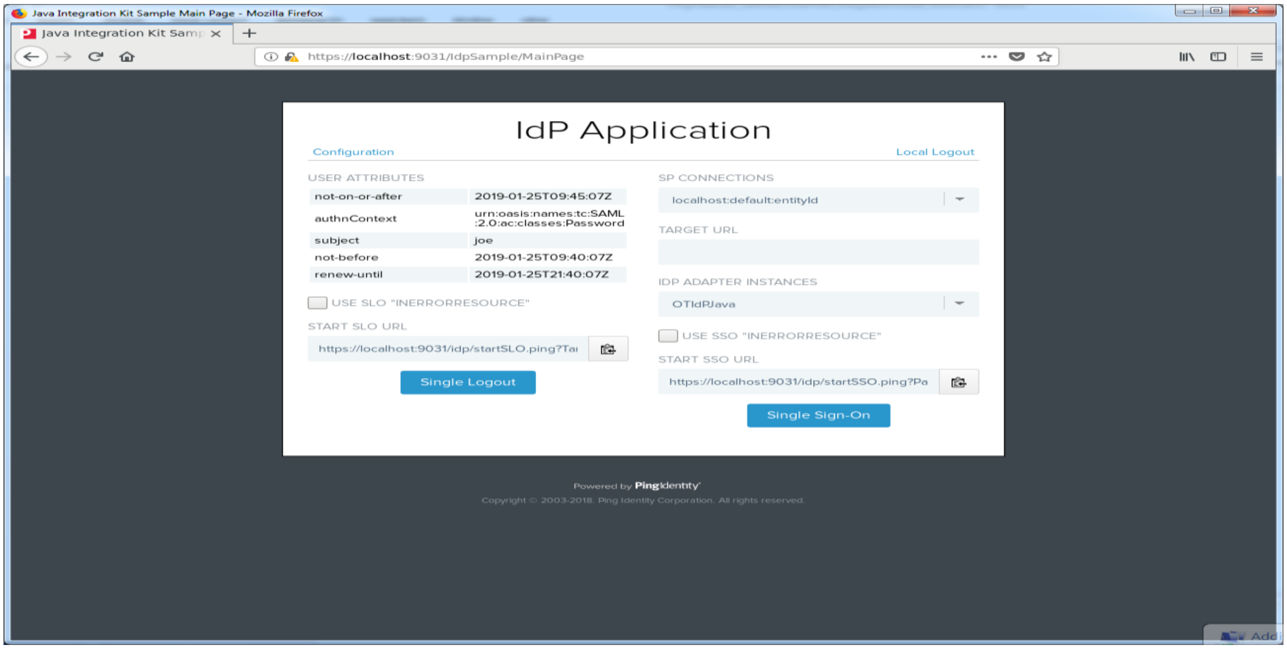
□ USE SSO "INERRORRESOURCE"

START SSO URL: https://localhost:9031/idp/startSSO.ping?Pa

Copyright © 2003-2018. Ping Identity Corporation. All rights reserved.

24. Click on **Local Login**. Enter credentials (joe/test) and click **Login**.

After login you will be able to see the user attributes for Idp Application.


Java Integration Kit Sample Main Page - Mozilla Firefox
Java Integration Kit Samp
https://localhost:9031/IdpSample/MainPage
IdP Application
Configuration
Local Logout
Single Logout
Single Sign-On
Powered by PingIdentity
Copyright © 2003-2018. Ping Identity Corporation. All rights reserved.

USER ATTRIBUTES

not-on-or-after	2019-01-25T09:45:07Z
authnContext	urn:oasis:names:tc:SAML:2.0:ac:classes:Password
subject	joe
not-before	2019-01-25T09:40:07Z
renew-until	2019-01-25T21:40:07Z

□ USE SLO "INERRORRESOURCE"

START SLO URL: https://localhost:9031/idp/startSLO.ping?Tar

SP CONNECTIONS: localhost:default:entityId

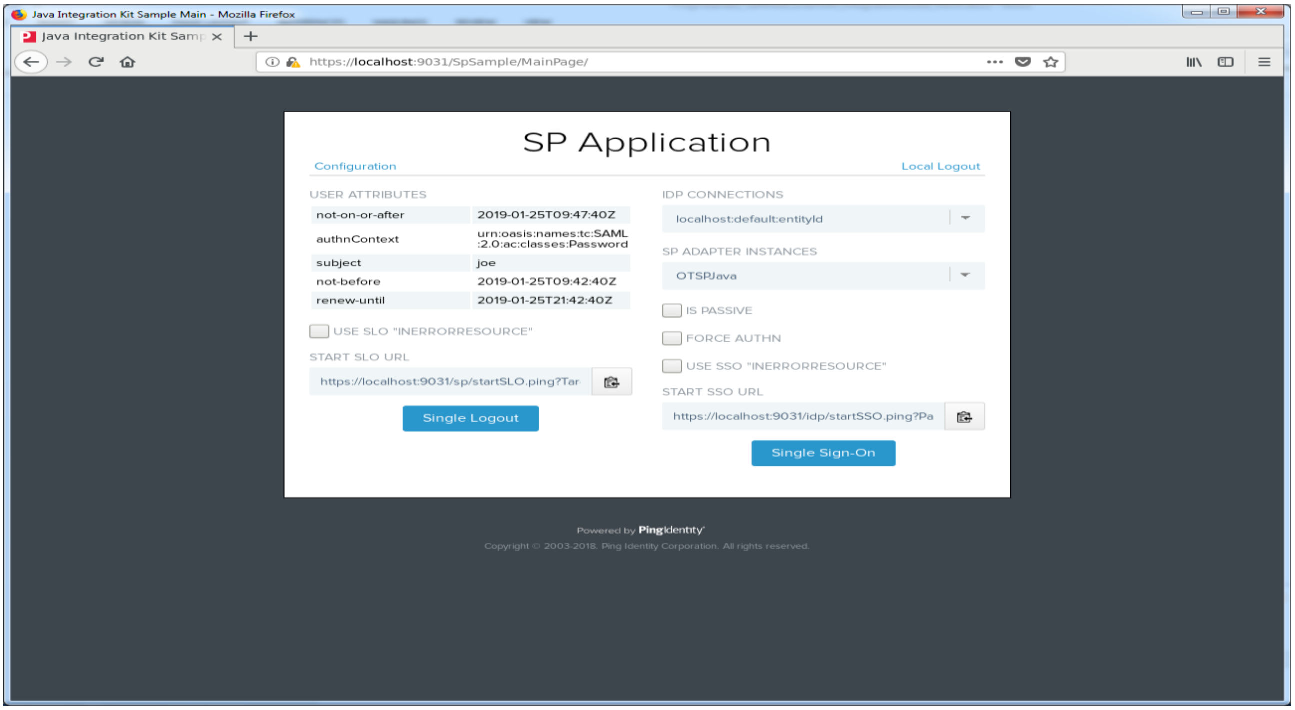
TARGET URL:

IDP ADAPTER INSTANCES: OTIdPJava

□ USE SSO "INERRORRESOURCE"

START SSO URL: https://localhost:9031/idp/startSSO.ping?Pa

25. Click on **Single Sign-On** and you will be automatically logged in SP application without any credential using SSO.


Java Integration Kit Sample Main - Mozilla Firefox
Java Integration Kit Samp
https://localhost:9031/SpSample/MainPage/
SP Application
Configuration
Local Logout
Single Logout
Single Sign-On
Powered by PingIdentity
Copyright © 2003-2018. Ping Identity Corporation. All rights reserved.

USER ATTRIBUTES

not-on-or-after	2019-01-25T09:47:40Z
authnContext	urn:oasis:names:tc:SAML:2.0:ac:classes:Password
subject	joe
not-before	2019-01-25T09:42:40Z
renew-until	2019-01-25T21:42:40Z

□ USE SLO "INERRORRESOURCE"

START SLO URL: https://localhost:9031/sp/startSLO.ping?Tar

IDP CONNECTIONS: localhost:default:entityId

SP ADAPTER INSTANCES: OTSPJava

□ IS PASSIVE

□ FORCE AUTHN

□ USE SSO "INERRORRESOURCE"

START SSO URL: https://localhost:9031/idp/startSSO.ping?Pa

This verifies the PingFederate SSO feature is working and that any tokens generated by the application are using the signing and decryption keys from the SafeNet HSM.