SafeNet Authentication Service
Integration Guide

Using SafeNet Authentication Service as an Identity Provider for OpenIAM
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.

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

**Document Part Number:** 007-013481-001, Rev. A

**Release Date:** April 2016
Contents

Third-Party Software Acknowledgement........................................................................................................... 4
Description .............................................................................................................................................................. 4
Applicability ............................................................................................................................................................ 4
Environment ............................................................................................................................................................ 5
Audience .................................................................................................................................................................. 5
SAML Authentication using SafeNet Authentication Service Cloud ................................................................. 5
SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication
Service-PCE .......................................................................................................................................................... 5
SAML Authentication Flow using SafeNet Authentication Service ................................................................. 6
SAML Prerequisites ................................................................................................................................................ 6
Configuring OpenIAM........................................................................................................................................... 6
   Creating a Service Provider .................................................................................................................................. 7
   Downloading the OpenIAM Metadata ................................................................................................................ 10
   Creating an Identity Provider .................................................................................................................................. 12
Downloading the SafeNet Authentication Service Metadata ............................................................................. 15
Configuring SafeNet Authentication Service ................................................................................................. 15
   Synchronizing Users Stores to SafeNet Authentication Service .................................................................. 15
   Assigning an Authenticator in SafeNet Authentication Service .................................................................. 15
   Adding OpenIAM as a Service Provider (SP) in SafeNet Authentication Service ........................................ 16
   Enabling SAML Services in SafeNet Authentication Service ........................................................................ 19
Running the Solution .......................................................................................................................................... 23
Appendix: Assigning a Service Provider (as the Default Resource) to OpenIAM Users for SSO ............... 25
Support Contacts .................................................................................................................................................... 29
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as OpenIAM.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

OpenIAM is a comprehensive Identity and Access Management infrastructure that provides a strong security foundation to provision users and authenticate and authorize access to enterprise systems.

OpenIAM is an integration of OpenIAM Identity Manager and OpenIAM Access Manager.

OpenIAM Identity Manager automates the task of managing identities across the various devices and applications used by the enterprise. OpenIAM Access Manager integrates seamlessly with OpenIAM Identity Manager to provide a comprehensive solution that allows you take control of not only who can access your systems, but what they can do once they are in there.

This document describes how to:

- Deploy multifactor authentication (MFA) options in OpenIAM using SafeNet OTP authenticators managed by SafeNet Authentication Service.
- Configure SAML authentication in OpenIAM using SafeNet Authentication Service as an identity provider.

It is assumed that the OpenIAM environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

OpenIAM can be configured to support multi-factor authentication in several modes. The SAML authentication will be used for the purpose of working with SafeNet Authentication Service.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet’s cloud-based authentication service
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version that is used by Service providers to deploy instances of SafeNet Authentication Service
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version that is used to deploy the solution on-premises in the organization
Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**
- **OpenIAM—Version 3.3.3**

Audience

This document is targeted to system administrators who are familiar with OpenIAM, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

SAML Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service (SAS) Cloud provides a service for SAML authentication that is already implemented in the SAS Cloud environment and can be used without any installation.

SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service (SAS) comes with two on-premises versions:

- **SafeNet Authentication Service – Service Provider Edition (SPE)**—An on-premises version of SafeNet Authentication Service targeted at service providers interested in hosting SAS in their data center.
- **SafeNet Authentication Service – Private Cloud Edition (PCE)**—An on-premises version of SafeNet Authentication Service targeted at organizations interested in hosting SAS in their private cloud environment.

For both on-premises versions, SAS can be integrated with the Shibboleth infrastructure, which uses a special on-premises agent called SafeNet Authentication Service Agent for Shibboleth.

For more information on how to install and configure the SafeNet Authentication Service Agent for Shibboleth, refer to the [SafeNet Support Portal](#).
SAML Authentication Flow using SafeNet Authentication Service

SafeNet Authentication Service (SAS) communicates with a large number of service providers and cloud-based services solutions using the SAML protocol.

The image below describes the dataflow of a multi-factor authentication transaction for OpenIAM.

1. A user attempts to log on to OpenIAM. The user is redirected to SafeNet Authentication Service (SAS). SAS collects and evaluates the user's credentials.
2. SAS returns a response to OpenIAM, accepting or rejecting the user’s authentication request.

SAML Prerequisites

To enable SafeNet Authentication Service to receive SAML authentication requests from OpenIAM, ensure the following:

- End users can authenticate from the OpenIAM environment with a static password.
- End users must be assigned a service provider as the default resource to achieve SSO (Refer to “Appendix: Assigning a Service Provider (as the Default Resource) to OpenIAM Users for SSO” on page 25).
- OpenIAM must be deployed on either the Jboss application server or Apache Tomcat server.

Configuring OpenIAM

Adding SafeNet Authentication Service (SAS) as an identity provider in OpenIAM requires the following:

- Creating a Service Provider, page 7
- Downloading the OpenIAM Metadata, page 10
- Creating an Identity Provider, page 12
Creating a Service Provider

A service provider offers services that access protected resources and handles authorization.

1. In a web browser, open the following URL:
   

   where, FQDN_of_client_machine is the domain name of the client machine, and 9080 is the default JBoss server port number.

2. On the OpenIAM login window, enter the administrator login ID and password, and then click Login.

![OpenIAM Login Window](image)

(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)


![OpenIAM Administrative Console](image)

(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)
4. On the **Authentication Providers** window, in the left pane, click **Create New Provider**.

![Authentication Providers window](image1)

(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)

5. On the **Create a New Authentication Provider** window, in the right pane, select **SAML Service Provider**.

![Create a New Authentication Provider window](image2)

(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)
6. On the **Create SAML Service Provider** window, in the right pane, complete the following fields, and then click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider Name</td>
<td>Enter a name for the service provider (for example, <strong>SAS_SP</strong>).</td>
</tr>
<tr>
<td>Linked to Managed System</td>
<td>Select a managed system (identity repository) (for example, <strong>OPENIAM</strong>).</td>
</tr>
<tr>
<td>SAML Issuer Name</td>
<td>Enter a request issuer name (for example, <code>http://&lt;IP address of the OpenIAM machine&gt;/idp/SAMLLogin.html</code>).</td>
</tr>
<tr>
<td>Sign-in page URL</td>
<td>Enter the SAML login page URL (for example, <code>https://idp1.cryptocard.com/idp/profile/SAML2/Redirect/SSO</code>).</td>
</tr>
<tr>
<td>Sign-out page URL</td>
<td>Enter the SAML logout page URL (for example, <code>https://idp1.cryptocard.com/idp/signout.jsp</code>).</td>
</tr>
</tbody>
</table>

(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)
On the **Authentication Providers** window, in the right pane, the newly created service provider (for example, **SAS_SP**) is listed.

![Authentication Providers Window](image)

*(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)*

## Downloading the OpenIAM Metadata

1. On the OpenIAM Administrative console window, click **Access Control > Authentication Providers**.

![OpenIAM Administrative Console](image)

*(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)*
2. On the Authentication Providers window, in the right pane, in the Name column, click on the newly created service provider (for example, SAS_SP).

3. On the Edit SAML Service Provider window, at the bottom, click SAML Metadata.
4. In a web browser, the metadata will be displayed. Copy the metadata and then save it as an XML document in your local drive.

Creating an Identity Provider

An identity provider stores and serves identity profiles and handles authentication.

1. On the OpenIAM Administrative console window, click **Access Control > Authentication Providers**.

2. On the **Authentication Providers** window, in the left pane, click **Create New Provider**.

(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)
3. On the **Create a New Authentication Provider** window, in the right pane, select **SAML IDP Provider**.

(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)
4. On the **Create SAML IDP Provider** window, complete the following fields, and then click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider Name</td>
<td>Enter a name for the provider (for example, SAS_IDP).</td>
</tr>
<tr>
<td>Linked to Managed System</td>
<td>Select a managed system (identity repository) (for example, OPENIAM).</td>
</tr>
<tr>
<td>Sign Response</td>
<td>Select NO.</td>
</tr>
<tr>
<td>Request Issuer</td>
<td>Enter the issuer of SAML requests (for example, http://&lt;IP of OpenIAM machine&gt;/idp/SAMLLogin.html).</td>
</tr>
<tr>
<td>Response Issuer</td>
<td>Enter the issuer of the SAML responses (entity ID of SAS, for example, <a href="https://idp1.cryptocard.com/idp/shibboleth">https://idp1.cryptocard.com/idp/shibboleth</a>).</td>
</tr>
<tr>
<td>Assertion Consumer URL</td>
<td>Enter the assertion consumer URL of OpenIAM (for example, <a href="http://localhost:9080/idp/sp/login">http://localhost:9080/idp/sp/login</a>).</td>
</tr>
</tbody>
</table>

(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)
Downloading the SafeNet Authentication Service Metadata

Browse to the https://idp1.cryptocard.com/idp/shibboleth URL. The SafeNet Authentication Service (SAS) metadata will be downloaded automatically. Save it locally on your machine.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with OpenIAM using SAML authentication requires:

- Synchronizing Users Stores to SafeNet Authentication Service, page 15
- Assigning an Authenticator in SafeNet Authentication Service, page 15
- Adding OpenIAM as a Service Provider (SP) in SafeNet Authentication Service, page 16
- Enabling SAML Services in SafeNet Authentication Service, page 19

Synchronizing Users Stores to SafeNet Authentication Service

Before SafeNet Authentication Service (SAS) can authenticate any user in your organization, you need to create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time using the Create User shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory/LDAP server using the SAS Synchronization Agent

For further details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the SafeNet Authentication Service Subscriber Account Operator Guide:


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Assigning an Authenticator in SafeNet Authentication Service

SafeNet Authentication Service (SAS) supports a number of authentication methods that can be used as a second authentication factor for users authenticating through OpenIAM.

The following authenticators are supported:

- eToken PASS
- RB-1 keypad token
- KT-4 token
- SafeNet GOLD
Authenticators can be assigned to users in two ways:

- **Manual provisioning**—Assign an authenticator to users one at a time.
- **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to “Provisioning” in the **SafeNet Authentication Service - Subscriber Account Operator Guide** to learn how to provision the different authentication methods to the users in the SAS user store.


**Adding OpenIAM as a Service Provider (SP) in SafeNet Authentication Service**

Add a service provider entry in the SafeNet Authentication Service (SAS) **SAML Service Providers** module to prepare it to receive SAML authentication requests from OpenIAM. You will need the metadata of OpenIAM.

**To add OpenIAM as a Service Provider in SafeNet Authentication Service (SAS):**
1. Log in to the SafeNet Authentication Service console with an Operator account.
2. Click the **COMMS** tab, and then click **SAML Service Providers**.

3. In the **SAML Service Providers** module, click the **SAML 2.0 Settings** link.

4. Click **Add**.
5. In the **Add SAML 2.0 Settings** section, complete the following fields, and then click **Apply**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Friendly Name</strong></td>
<td>Enter the OpenIAM name.</td>
</tr>
<tr>
<td><strong>SAML 2.0 Metadata</strong></td>
<td>Select <strong>Upload Existing Metadata File</strong>. Click <strong>Choose File</strong>, select the service provider’s metadata file, and then click <strong>Open</strong>.</td>
</tr>
</tbody>
</table>

![Add SAML 2.0 Settings](image)

**NOTE:** The remaining options are used to customize the appearance of the logon page presented to the user. For more information on logon page customization, refer to “Configure SAML Service” in the **SAML Configuration Guide**:

OpenIAM is added as a service provider in the system.

![SAMl Service Providers](image)
Enabling SAML Services in SafeNet Authentication Service

After OpenIAM has been added to SafeNet Authentication Service (SAS) as a service provider, the users should be granted permission to use this service provider with SAML authentication.

There are two methods to enable the user to use the service provider:

- Manually, one user at a time, using SAML Services module
- Automatically, by defining groups of users, using SAML Provisioning Rules

Using the SAML Services Module

Manually enable a single user to authenticate against one or more configured SAML service providers.

1. Log in to the SAS console with an Operator account.

2. Click the ASSIGNMENT tab, and then search for the required user.
3. Click the appropriate user in the **User ID** column.

4. Click **SAML Services**.

5. Click **Add**.
6. Under **Add SAML Service**, do the following:
   a. From the **Service** menu, select the OpenIAM service provider.
   b. In **SAML Login ID** field, select the type of login ID (User ID, E-mail, or Custom) to be sent as a UserID to OpenIAM in the response.
   c. Click **Add**.

   ![Add SAML Service](image)

   The user can now authenticate to OpenIAM using SAML authentication.

   ![SAML Services](image)

**Using SAML Provisioning Rules**

Use this module to enable groups of users to authenticate to SAML service providers.

1. Log in to the SafeNet Authentication Service (SAS) console with an Operator account.

![SafeNet Authentication Service](image)
2. Click the **POLICY** tab, and then click **Automation Policies**.

3. Click the **SAML Provisioning Rules** link.

4. Click **New Rule**.
5. Configure the following fields, and then click Add:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rule Name</strong></td>
<td>Enter a name for the rule.</td>
</tr>
<tr>
<td><strong>User is in container</strong></td>
<td>Users affected by this rule must be in the selected container.</td>
</tr>
<tr>
<td><strong>Groups</strong></td>
<td>The Virtual Server groups box lists all groups. Click the user groups that will be affected by the rule, and then click the right arrow to move it to the Used by rule box.</td>
</tr>
<tr>
<td><strong>Parties</strong></td>
<td>The Relying Parties box lists all service providers. Click the service providers that the groups of users will authenticate to, and then click the right arrow to move it to Rule Parties box.</td>
</tr>
<tr>
<td><strong>SAML Login ID</strong></td>
<td>Select User ID. The User ID will be returned to the service provider in the SAML assertion.</td>
</tr>
</tbody>
</table>

![Image of the SafeNet Authentication Service interface](image)

### Running the Solution

For this integration, the SafeNet GrIDsure token is configured for authentication with the SAS solution. Before running the solution, ensure that the JBoss server is running on the client machine.

1. In a web browser, open the following URL:

   http://<domain or localhost or ip of OpenIAM Machine>/idp/sp/login?issuer=SAMLIssuerNameFromAbove

2. You will be redirected to the SAS login page. In the **User Name** field, enter your user name, and then click **Login**.

   ![Login Screen](image)

3. In the **Password** field, enter your Personal Identification Pattern (PIP), and then click **Login**.

   ![Login Screen](image)
After successful authentication, you will be able to access the OpenIAM console.

(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)

Appendix: Assigning a Service Provider (as the Default Resource) to OpenIAM Users for SSO

1. On the OpenIAM Administrative console window, click **Access Control > Resource**.

(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)
2. On the **Search Resources** window, in the **Resource Name** column, click on the service provider (for example, **SAS_SP**) that you created earlier in step 6 of “Creating a Service Provider” on page 7.

![Search Resources](image1.png)

*(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)*

3. On the **Edit Resource** window, in the **URL** field, enter the self-service URL (for example, **http://localhost:9080/selfservice**), and then click **Save**.

![Edit Resource](image2.png)

*(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)*

4. In the left pane, click **Entitlements**.
5. On the **Children of Resource** window, in the right pane, click **Entitled Users**.

![Image of Children of Resource window](image1.png)

*(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)*

6. On the **Entitled Users to Resource** window, in the right pane, click **Add User**.

![Image of Entitled Users to Resource window](image2.png)

*(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)*

7. Under **Search Users**, in the **Last name** or **Email Address** field, enter the last name or email address of the user, respectively, and then click **Search**.

![Image of Search Users](image3.png)

*(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)*
8. In the second table, in the **Name** column, click on the OpenIAM user name (for example, **alice al**).

![OpenIAM User List]

(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)

The user is listed in the first table with **User status** as **ACTIVE**.

![OpenIAM User List]

(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)
Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read 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.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Gemalto, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>