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 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: 007-013524-001, Rev. A
Release Date: June 2016
## Contents

Third-Party Software Acknowledgement ................................................................. 4
Description ................................................................................................................. 4
Applicability .................................................................................................................. 4
Environment ............................................................................................................... 4
Audience ...................................................................................................................... 5
SAML Authentication using SafeNet Authentication Manager .............................. 5
Authentication Flow using SafeNet Authentication Manager ................................... 5
SAML Prerequisites .................................................................................................... 5
Configuring SafeNet Authentication Manager .......................................................... 6
  Synchronizing User Stores to SafeNet Authentication Manager ............................... 6
  Assigning Tokens in SafeNet Authentication Manager .............................................. 6
  Configuring SafeNet Authentication Manager as an Identity Provider ..................... 7
  Configuring SafeNet Authentication Manager for SAML-based User Federation .. 9
Configuring OpenIAM ................................................................................................. 12
  Creating a Service Provider .................................................................................... 12
  Creating an Identity Provider .................................................................................. 16
Running the Solution .................................................................................................. 19
Appendix: Assigning a Service Provider (as the Default Resource) to OpenIAM Users for SSO .... 21
Support Contacts ....................................................................................................... 24
**Third-Party Software Acknowledgement**

This document is intended to help users of Gemalto 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 Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

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 multi-factor authentication (MFA) options in OpenIAM using SafeNet tokens managed by SafeNet Authentication Manager.
- Configure SAML authentication in OpenIAM using SafeNet Authentication Manager 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 Manager.

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 Manager.

**Applicability**

The information in this document applies to:

- **SafeNet Authentication Manager**—A server version of SAM 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 Manager Version**—Version 8.2 HF 710
- **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 Manager (SAM).

SAML Authentication using SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) provides a SAML authentication option that is already implemented in the SAM environment and can be used without any installation.

Authentication Flow using SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) 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 Manager (SAM). SAM collects and evaluates the user’s credentials.
2. SAM returns a response to OpenIAM, accepting or rejecting the user’s authentication request.

SAML Prerequisites

To enable SafeNet Authentication Manager (SAM) 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 21).

• OpenIAM must be deployed on either the Jboss application server or Apache Tomcat server (in this solution, Jboss server is used).

Configuring SafeNet Authentication Manager

Using SafeNet Authentication Manager (SAM) as an identity provider for OpenIAM requires the following:

• Synchronizing User Stores to SafeNet Authentication Manager, page 6
• Assigning Tokens in SafeNet Authentication Manager, page 6
• Configuring SafeNet Authentication Manager as an Identity Provider, page 7
• Configuring SafeNet Authentication Manager for SAML-based User Federation, page 9

Synchronizing User Stores to SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) manages and maintains tokens information in its data store, including the tokens status and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

• Novell eDirectory
• Microsoft ADAM/AD LDS
• OpenLDAP
• Microsoft SQL Server 2005 and 2008
• IBM Lotus Domino
• IBM Tivoli Directory Server

Assigning Tokens in SafeNet Authentication Manager

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

The following tokens are supported:

• eToken PASS
• eToken NG-OTP
• SafeNet GOLD
• SMS tokens
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
- SafeNet Mobile Authentication (iOS)
- SafeNet eToken 3400
- SafeNet eToken 3500

Tokens can be assigned to users as follows:

- **SAM Management Center**—Management site used by SAM administrators and helpdesk personnel for token enrollment and lifecycle management.
- **SAM Self-Service Center**—Self-service site used by end users for managing their tokens.
- **SAM Remote Service**—Self-service site used by employees not on the organization’s premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet’s tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

### Configuring SafeNet Authentication Manager as an Identity Provider

To use OpenIAM as a service provider and SafeNet Authentication Manager (SAM) as an identity provider, SAM must be configured as an identity provider.

1. From the Windows Start menu, click Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager.

![Configuration Manager](image)

*(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)*
2. Click the **Action** tab, and then select **Cloud Configuration**.

![SafeNet Authentication Manager - Configuration Manager](image1)

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

3. On the **Info for Service Provider** tab, in the **Domain URL** field, enter the web address of the SAM portal server.

![Cloud Settings](image2)

The remaining fields are generated according to the Domain URL that was entered.
4. Click OK.
5. Copy and paste the values of the **Sign-in page URL**, **Sign-out page URL**, and **Change password URL** fields in a text file.

### Configuring SafeNet Authentication Manager for SAML-based User Federation

SafeNet Authentication Manager’s Token Policy Object (TPO) policies include application authentication settings for SAML service providers. These settings are used by SAM’s portal to communicate with service providers.

For general portal configuration, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

**To edit the TPO for SAM’s portal configuration:**

1. Open the **Token Policy Object Editor** window for the appropriate group. See the *SafeNet Authentication Manager 8.2 Administrator’s Guide* for more information.

2. In the left pane, click **Protected Application Settings > User Authentication**.

![Token Policy Object Editor](image)

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

3. In the right pane, double-click **Application Authentication Settings**.
4. On the **Application Authentication Settings Properties** window, perform the following steps:
   a. Select **Define this policy setting**.
   a. Select **Enabled**.
   b. Click **Definitions**.

   ![Application Authentication Settings Properties](image1)

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

5. On the **Application Authentication Settings** window, in the left pane, right-click **Application Authentication Settings**, and then select **Create a new profile**.

   ![Application Authentication Settings](image2)

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

6. In the left pane, right-click the new profile, and then rename it to a user-friendly name (for example, **OpenIAM**).
7. In the left pane, click the new profile.

8. In the right pane, double-click on the following policies, and enter the appropriate information:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Policy Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application issuer</td>
<td>Not Defined</td>
</tr>
<tr>
<td>SAM issuer</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Application's login URL</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Audience URI</td>
<td>Not Defined</td>
</tr>
<tr>
<td>User mapping</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Automatic Windows authentication</td>
<td>Not Defined</td>
</tr>
<tr>
<td>OTF authentication</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Certificate-based authentication</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Network password authentication</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Always require authentication</td>
<td>Not Defined</td>
</tr>
<tr>
<td>End SSO session upon sign-out</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Context based authentication</td>
<td>Not Defined</td>
</tr>
</tbody>
</table>

**Application Issuer**: Enter the Entity ID of OpenIAM.

**SAM issuer**: A unique SAM ID to be identified in SAML authentication (for example, SAM)

**Application’s login URL**: Enter the ACS URL of OpenIAM.

**Audience URI**: Enter the Entity ID of OpenIAM.

**User mapping**: Select **Email**.

---

**NOTE**: Various details for this table can be found in the metadata of OpenIAM (Page 19, Step 11).

The following is an example of the completed policy settings in the Application Authentication Settings window:

![Application Authentication Settings window](image)

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

10. Click OK until all of the Token Policy Object Editor windows are closed.

**Configuring OpenIAM**

Adding SafeNet Authentication Manager (SAM) as an identity provider in OpenIAM requires the following:

- Creating a Service Provider, page 12
- Creating an Identity Provider, page 16

**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**.

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

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

   (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.

5. On the Create a New Authentication Provider window, in the right pane, select SAML Service Provider.
6. On the **Create SAML Service Provider** window, in the right pane, complete the following fields, and then click **Save**.

<table>
<thead>
<tr>
<th><strong>Provider Name</strong></th>
<th>Enter a name for the service provider (for example, SAS_SP).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Linked to Managed System</strong></td>
<td>Select a managed system (identity repository) (for example, OPENIAM).</td>
</tr>
<tr>
<td><strong>SAML Issuer Name</strong></td>
<td>Enter a request issuer name (for example, http://&lt;IP address of the OpenIAM machine&gt;/idp/SAMLLogin.html).</td>
</tr>
<tr>
<td><strong>Sign-in page URL</strong></td>
<td>Enter the SAML login page URL (for example, <a href="http://10.164.44.158/samcloud/default.aspx">http://10.164.44.158/samcloud/default.aspx</a>).</td>
</tr>
<tr>
<td><strong>Sign-out page URL</strong></td>
<td>Enter the SAML logout page URL (for example, <a href="http://10.164.44.158/samcloud/logout.aspx">http://10.164.44.158/samcloud/logout.aspx</a>).</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.)*

### 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**.

![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 left pane, click **Create New Provider**.

   ![Authentication Providers Window](image1.png)

   *(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**.

   ![Create a New Authentication Provider Window](image2.png)

   *(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 SAM, for example, SAM).</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.)
Running the Solution

For this integration, the SafeNet eToken PASS is configured for authentication with the SafeNet Authentication Manager (SAM) solution. Before running the solution, ensure that JBoss Server is running on the client machine.

1. In a web browser enter the following URL to initiate SSO:

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


2. You will be redirected to the SAM login window. Enter your username, and then click OK.
3. On the **OTP Authentication** window, in the **OTP Authentication Code** field, enter the OTP (generated using SafeNet eToken PASS), and then click **OK**.

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**.

   ![OpenIAM Administrative Console Window](image)

   *(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 12.

   ![Search Resources Window](image)

   *(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**.

4. In the left pane, click **Entitlements**.

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

(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**.

![Add User](image1.jpg)

*(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**.

![Search Users](image2.jpg)

*(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](image3.jpg)

*(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**.

(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>
</table>
| **Address**             | Gemalto  
4690 Millennium Drive  
Belcamp, Maryland  21017 USA                                                      |
| **Phone**               | United States  
1-800-545-6608  
International  
1-410-931-7520 |
| **Technical Support**   | **Customer Portal**  
[https://serviceportal.safenet-inc.com](https://serviceportal.safenet-inc.com)  
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. |