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: 007-013585-001, Rev. A
Release Date: August 2016
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Oracle Access Manager R3.

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.

Oracle Access Manager delivers risk-aware end-to-end user authentication, single sign-on, and authorization protection, providing enterprises with secure access from mobile devices and seamless integration of social identities with applications. This document describes how to:

- Deploy multi-factor authentication (MFA) options in Oracle Access Manager R3 using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Deploy and configure Oracle Access Manager R3 using SAS agent for Oracle OAM R3.

It is assumed that the Oracle Access Manager R3 environment is already configured and working with LDAP passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Oracle Access Manager R3 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)**
- **SafeNet Authentication Service Agent** for Oracle Access Manager
  - **Supported Platforms**: RedHat 5.7 64 bit / RedHat 6.4 64 bit / Oracle Linux 64 bit
  - **Additional Software Components**: Java Runtime (JRE)
- Oracle Access Manager R3 installed on RHEL v6.4

**Audience**

This document is targeted to system administrators who are familiar with Oracle Access Manager R3, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

**SAS Authentication API Authentication using SafeNet Authentication Service Cloud**

The image below describes the environment required to implement an OAM R3 solution using SafeNet Authentication Service (SAS).

![Image of environment required for SAS Authentication API](image)

**SAS Authentication API 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.

**SAS API Authentication using SafeNet Authentication Service**

Gemalto SafeNet SAS OAM Agent is an MFA adapter that provides users a way to authenticate through OAM agent using SAS as a secondary authenticator.
The image below describes the dataflow of a multi-factor authentication transaction for Oracle Access Manager R3.

1. A user attempts to access a resource which is protected with Oracle Access Manager (OAM) R3.
2. OAM displays the SAS agent login page.
3. The user enters his or her credentials (for example, LDAP and OTP).
4. The SAS agent validates the LDAP credentials against the configured LDAP server.
5. After successful OTP validation, the user is redirected to access the protected resource.

## Configuring Oracle Access Manager R3 with SAS Agent

Configuring SAS agent on Oracle Access Manager R3 requires:

- Installing the SAS Agent Plugin, page 6
- Configuring the .ini File of the SAS Agent, page 7
- Importing the SAS Agent Plugin Using the Oracle Access Manager Console, page 7
- Creating an Authentication Module, page 10
- Creating Authentication Scheme, page 14
- Forcing the SAS Agent Authentication Scheme on a Protected Resource, page 16
- Configuring the WebLogic Server, page 17
- Deploying an Agent on the WebLogic Server, page 18

### Installing the SAS Agent Plugin

Install the SAS agent rpm.

1. Run the following command:
   
   ```bash
rpm –ivh cryptocard-oam-agent-[your installation build].x86_64.rpm
   ```
2. The installation package is installed at the `/usr/local/cryptocard` location.

![Image](image.png)

Configuring the .ini File of the SAS Agent

Modify the .ini file of the SAS agent by adding the BSID server details, protocol, etc. Configure the following variables in the `/usr/local/cryptocard/ini/JCryptoWrapper.ini` file:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PrimaryProtocol</td>
<td>Select <code>http/https</code>.</td>
</tr>
<tr>
<td>PrimaryServer</td>
<td>Enter the primary SAS server host.</td>
</tr>
<tr>
<td>PrimaryServerPort</td>
<td>Enter the port number (for example, <code>80/443</code>).</td>
</tr>
<tr>
<td>REDIRECT-LOCATION-AFTER-AUTHENTICATION</td>
<td>Enter the OAM redirection URL (For example, <code>http://iamdemo.oracle.com:14100/oam/server/auth_cred_submit</code>).</td>
</tr>
</tbody>
</table>

Importing the SAS Agent Plugin Using the Oracle Access Manager Console

1. Log in to the OAM Management portal as an administrator.
2. On the OAM Management portal, under **Plug-ins**, click **Authentication Plug-ins**.

![OAM Management Portal - Plug-ins](image)

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

3. Click **Import Plug-in**.

![OAM Import Plug-in](image)

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

4. The **Import Plug-in** window displayed. Click **Browse**.

![Import Plug-in](image)

*(The screen image above is from Oracle Access Manager. Trademarks are the property of their respective owners.)*
5. On the File Upload window, select the agent.jar file (for example, /usr/local/cryptocard/oam/war/CRYPTOCARDOamAuthModule.jar), and then click Open.


7. The SAS agent plugin is listed. Select the SAS agent plug-in, and then click Distribute Selected.

8. The Activation Status is change to Distributed.
9. Select the SAS agent plug-in, and then click **Activate Selected**. The **Activation Status** is changed to **Activated**.

![Oracle Access Manager](image)

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

**Creating an Authentication Module**

Configure the authentication module that defines the type and order of the authentication. In the authentication module, you configure the OTP and LDAP authentication that will be used by the SAS agent.

1. On the OAM Management portal, under **Plug-ins**, click **Authentication Modules**.

![Oracle Access Manager](image)

*(The screen image above is from Oracle Access Manager. Trademarks are the property of their respective owners.)*
2. Click Create Authentication Module > Create Custom Authentication Module.

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

3. On the Authentication Module window, on the General tab, complete the following fields:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the module.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Enter a description for the module.</td>
</tr>
</tbody>
</table>

(The screen image above is from Oracle Access Manager. Trademarks are the property of their respective owners.)
4. Click the **Steps** tab, and then click the **+** icon to add a new step to the authentication module.

![Oracle Access Manager Screenshot](image)

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

5. Perform the following three steps:
   a. On the **Add new step** window, for **OTP**, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Step Name</th>
<th>Enter a name for the module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plug-in Name</td>
<td>Select <strong>CRYPTOCARDOAMAuthModule</strong>.</td>
</tr>
</tbody>
</table>

   *(The screen image above is from Oracle Access Manager. Trademarks are the property of their respective owners.)*
b. For **User Identification** (LDAP Identification), complete the following fields, and the click **OK**.

<table>
<thead>
<tr>
<th>Step Name</th>
<th>Enter a name to the module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plug-in Name</td>
<td>Select <strong>UserIdentificationPlugin</strong>.</td>
</tr>
</tbody>
</table>

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

c. For **User Authentication** (LDAP Authentication), complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Step Name</th>
<th>Enter a name to the module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plug-in Name</td>
<td>Select <strong>UserAuthenticationPlugin</strong>.</td>
</tr>
</tbody>
</table>

(The screen image above is from Oracle Access Manager. Trademarks are the property of their respective owners.)
6. Click the **Steps Orchestration** tab, and then in the **Initial Step** field, select **OTP** to be the first step you added (refer to step 6 a), and then fill the steps as follows.

![SafeNet Authentication Service](image)

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

7. Click **Apply**.

## Creating Authentication Scheme

Create the authentication scheme that will use the authentication module that is created in the previous section.

1. On the OAM Management portal, under **Access Manager**, click **Authentication Schemes**.

![Oracle Access Manager](image)

*(The screen image above is from Oracle Access Manager. Trademarks are the property of their respective owners.)*
2. Click **Create Authentication Scheme**.

![Create Authentication Scheme](image)

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

3. Complete the following fields, and then click **Apply**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the authentication scheme.</td>
</tr>
<tr>
<td>Authentication Level</td>
<td>Select 2.</td>
</tr>
<tr>
<td>Challenge Method</td>
<td>Select FOAM.</td>
</tr>
<tr>
<td>Challenge Redirect URL</td>
<td>Enter <code>/oam/server/</code></td>
</tr>
<tr>
<td>Authentication Module</td>
<td>Select the authentication module (for example, <strong>SAS Agent</strong>) that you created earlier in step 3 of “Creating an Authentication Module” on page 10.</td>
</tr>
<tr>
<td>Challenge URL</td>
<td>Enter the URL of the credentials collector (for example, <a href="http://oamserver1.localdomain:14100/Login/Login.jsp">http://oamserver1.localdomain:14100/Login/Login.jsp</a>).</td>
</tr>
<tr>
<td>Context Type</td>
<td>Select external.</td>
</tr>
</tbody>
</table>

![Authentication Scheme](image)

(The screen image above is from Oracle Access Manager. Trademarks are the property of their respective owners.)
Forcing the SAS Agent Authentication Scheme on a Protected Resource

Force the SAS agent authentication scheme on the protected resource in OAM.

1. On the OAM Management portal, under Access Manager, click Application Domains.

   ![Application Domains](image1)

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

2. Click Search, and then under Search Results, click on the protected resource (for example, oamserverps3gate).

   ![Search Results](image2)

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

4. In the Authentication Scheme field, select the authentication scheme (for example, SAS Agent), and then click Apply.

Configuring the WebLogic Server

Add the LD_LIBRARY_PATH to the WebLogic Server (WLS) using SSH.

1. Log in to your Linux server hosting WLS using SSH.
2. Add LD_LIBRARY_PATH to the WLS startup scripts at the following locations:
   a. In the <WLS INSTALL PATH>/oracle/Middleware/wlserver_xx/common/bin/commEnv.sh file, at the end, just before resetFD, add the following, and then save the file.

   ```
   LD_LIBRARY_PATH=/user/local/cryptocard/oam/bin/x64:{LD_LIBRARY_PATH}
   export LD_LIBRARY_PATH
   ```
b. In the `<WLS INSTALL PATH>/oracle/Middleware/user_projects/domains/OAMdomain/bin/setDomainEnv.sh` file, at the end, just after `export BEA_JAVA_HOME`, add the following, and then save the file.

```bash
LD_LIBRARY_PATH=/user/local/cryptocard/oam/bin/x64:{LD_LIBRARY_PATH}
export LD_LIBRARY_PATH
```

3. Restart the OAM and WLS services.

### Deploying an Agent on the WebLogic Server

Deploy the agent `.war` file on the WebLogic Server (WLS).

1. Log in to the WLS web interface.

   ![WebLogic Server Interface](image)

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

2. In the left pane, under **Domain Structure**, click **Deployments**, and then in the right pane, click **Install**.

   ![Deployments Page](image)

   *(The screen image above is from Oracle Access Manager. Trademarks are the property of their respective owners.)*
3. On Install Application Assistant, select the CRYPTOCardOamLogin.war file from the agent installation folder (/usr/local/cryptocard/oam/war/), and then click Next.

4. Under Choose targeting style, select Install this deployment as an application, and then click Next.
5. Under **Select deployment targets**, select the OAM server, and then click **Next**.

![Screenshot of Oracle WebLogic Server Administration Console](image1)

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

6. Under **Optional Settings**, do not change the default configuration. Click **Finish**.

![Screenshot of Oracle Application Assistant](image2)

*(The screen image above is from Oracle Access Manager. Trademarks are the property of their respective owners.)*
7. In the left pane, under **Domain Structure**, click **Deployments**. Then, in the right pane under **Deployments**, validate if the **State** of the **CRYPTOCardOamLogin** agent is **Active**.

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

### Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with Oracle Access Manager R3 using SAML authentication requires:

- Creating Users Stores in SafeNet Authentication Service, page 21
- Assigning an Authenticator in SafeNet Authentication Service, page 22
- Configuring SafeNet Authentication Service Auth Node and Downloading the Encryption Key, page 22

### Creating Users Stores in 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 additional 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 who are authenticating through Oracle Access Manager R3.

The following authenticators are supported:

- eToken PASS
- RB-1 keypad token
- KT-4 token
- SafeNet GOLD
- SMS tokens
- MP-1 software token
- GrIDsure
- MobilePASS

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 Rules” 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.


Configuring SafeNet Authentication Service Auth Node and Downloading the Encryption Key

In the event that the SafeNet Authentication Service (SAS) server is not installed on the same machine as AD and ADFS, the following steps must be performed:

1. Log in to the SafeNet Authentication Service console as the account operator.
2. Click Virtual Servers > Comms > Authentication Processing.
3. Click the Authentication Agent Settings link, and then click Download to download the encryption key file.

4. Click Virtual Servers > Comms > Auth Nodes.

5. Click the Auth Nodes link, and then click Add.

6. Complete the following fields, and then click Save.

   - **Agent Description**: Type a description for this node (for example, DC).
   - **Host Name**: Type a host name.
   - **Low IP Address In Range**: Type the low IP address.
   - **High IP Address In Range**: Type the high IP address. (The low and high IP addresses may be the same since the node is referencing a single machine.)
   - **Exclude from PIN change requests**: Do not select this check box.

The authentication node is added to the system.
Running the Solution

Once the configurations are done, log in to the protected resource and test the solution.

1. In a web browser, go to the protected resource.
2. You will be redirected to the SafeNet Authentication Service (SAS) login window. Enter your user name, LDAP password, and one-time password (OTP), and then click **Login**.

After successful authentication you will be redirected to the protected resource

Appendix: Troubleshooting

The following issues can occur during the integration:

- Setting File and Directory Permissions, page 25
- WebLogic Server SSL Errors (SSL connection to SAS), page 25
- WebLogic Agent Deployment Error, page 26
- String Truncation, page 26
Setting File and Directory Permissions

Administrators must secure file and directory access permissions.

For example,

- The READONLY access permission must be set on the INI file for the WLS or OAM process owner. The Plugin and web applications will require READONLY permissions for the INI file, key file, and resource directory, as well as files in that directory.

- The WRITE access permission must be set on log directory for the WLS/OAM process owner.

WebLogic Server SSL Errors (SSL connection to SAS)

As the certificate policy is different in WebLogic than it is in a stand-alone Java program, it is advised to use a Sun implementation instead of WebLogic.

http://webtech-kapil.blogspot.com/2010/06/javalangclasscastexception.html

Start WebLogic with the following flag:

-\texttt{DUseSunHttpHandler=true}

The standard Sun SSL implementation will be used.

When SOAP transport in the INI file via Java code, on WLS, you might encounter SSL connection, certificate validation, and SSL handshake errors. These errors can be prevented by adding the following to your WLS startup script below the comments block:

\texttt{<WLS INSTALL PATH>/oracle/Middleware/user_projects/domains/OAMdomain/bin/setDomainEnv.sh}
WebLogic Agent Deployment Error

When deploying the agent on the Weblogic server (refer to Deploying an Agent on the WebLogic Server, on page 18), there could be an error (Java exception) which states that JCryptoWrapper cannot be loaded using the following installation path:

```
javax.servlet.ServletException: JCryptoWrapper loading FAILED using installation path[/usr/local/cryptocard/oam/bin/x64/libJCryptoWrapper.so] and System Path.
```

In this scenario, it is recommended to edit the following files and add the hardcoded path:

1. Edit the following files:
   
   `/etc/ld.so.conf.d`

   `-oracle/.bash_profile`

2. Add the following to both files:

   ```
   LD_LIBRARY_PATH=<OAM Agent Path>
   export LD_LIBRARY_PATH
   
   For example,
   
   LD_LIBRARY_PATH=/usr/local/cryptocard/oam/bin/x64/:${LD_LIBRARY_PATH}
   export LD_LIBRARY_PATH
   ```

3. Save both the files.
4. Restart the machine.

String Truncation

In OAM R3, by default, the maximum size of a parameter that can be sent to a custom plugin is 500 characters. This can cause an error message to appear after a successful authentication with SAS is done.

This is a data sanitization feature to control what OAM send to a 3rd part plugin.

In order to override the default parameter, perform the following steps:

1. Connect to the WLST admin CLI.
2. Run the following command:

   ```
   configTrustedInputs(name="safenet_data_N",maxSize="4000")
   ```

For more information, refer to the OAM R3 admin guide or Oracle Doc ID 2039164.1.
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**| 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. |