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.

© 2015 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:** 007-013235-001, Rev. B

**Release Date:** June 2016
Contents

Third-Party Software Acknowledgement ................................................................. 4
Description ................................................................................................................. 4
Applicability ............................................................................................................... 4
Environment ............................................................................................................. 4
Audience ..................................................................................................................... 5
SAML Authentication using SafeNet Authentication Service Cloud ......................... 5
SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE5
SAML Authentication Flow using SafeNet Authentication Service ............................ 5
SAML Prerequisites .................................................................................................. 6
Configuring Salesforce ............................................................................................... 6
  Downloading the SafeNet Authentication Service Metadata .................................. 6
  Download the SafeNet Identity Provider Certificate ............................................. 6
  Enabling SAML for Salesforce .............................................................................. 7
  Setting Single Sign-On for Salesforce ................................................................... 9
  Creating Users in Salesforce ................................................................................. 11
Configuring SafeNet Authentication Service ............................................................ 12
  Synchronizing Users Stores to SafeNet Authentication Service .......................... 12
  Assigning an Authenticator in SafeNet Authentication Service ............................ 13
  Adding Salesforce as a Service Provider (SP) in SafeNet Authentication Service ... 13
  Enabling SAML Services in SafeNet Authentication Service ............................... 16
Running the Solution ................................................................................................. 21
Support Contacts ....................................................................................................... 23
Third-Party Software Acknowledgement

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

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.

Salesforce is a cloud computing and social enterprise software-as-a-service (SaaS) provider. It is a top-notch CRM application built on the Force.com platform, and can manage all of the customer interactions in an organization through different media, such as phone calls, site email enquiries, and social media.

This document describes how to:

- Configure SAML authentication in Salesforce using SafeNet Authentication Service as an identity provider.

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

Salesforce 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 – Service Provider Edition (SAS-SPE)**
- **Salesforce** - Salesforce.com Developer Edition
**Audience**

This document is targeted to system administrators who are familiar with Salesforce, 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 Salesforce.

---

**SafeNet Authentication Service: Integration Guide**

Using SafeNet Authentication Service as an Identity Provider for Salesforce

Document PN: 007-013235-001, Rev. B, Copyright © 2016 Gemalto, Inc., All rights reserved.
1. A user attempts to log on to Salesforce. The user is redirected to SafeNet Authentication Service. SAS collects and evaluates the user's credentials.

2. SAS returns a response to Salesforce, accepting or rejecting the user's authentication request.

**SAML Prerequisites**

To enable SafeNet Authentication Service (SAS) to receive SAML authentication requests from Salesforce, ensure that the end users can authenticate from the Salesforce environment with a static password.

**Configuring Salesforce**

To add SafeNet Authentication Service (SAS) as an Identity Provider in Salesforce:

- Enabling SAML for Salesforce, page 7
- Setting Single Sign-On for Salesforce, page 9
- Creating Users in Salesforce, page 11

**Downloading the SafeNet Authentication Service Metadata**

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

**Download the SafeNet Identity Provider Certificate**

Browse to the [https://cloud.safenet-inc.com/console/cert/idp.crt](https://cloud.safenet-inc.com/console/cert/idp.crt) URL. The SafeNet identity provider certificate will automatically download. Save it locally on your machine.
Enabling SAML for Salesforce

1. Open a web browser and log in to the Salesforce URL (for example, https://login.salesforce.com/).
2. Enter your Username and Password, and then click Log in to Salesforce.

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

3. On the Salesforce1 Setup home page, click Setup in the upper-right corner of the window.

(The screen image above is from Salesforce®. Trademarks are the property of their respective owners.)
4. In the left pane, select **Administer > Security Controls > Single Sign-On Settings**.

![Image](image-url)

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

5. A **Critical Updates** message is displayed. Select **No**, and then click **OK** to proceed.

![Image](image-url)

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

6. On the **Single Sign-On Settings** window, select **SAML Enabled**, and then click **Save**.

![Image](image-url)

(The screen image above is from Salesforce®. Trademarks are the property of their respective owners.)
Setting Single Sign-On for Salesforce


2. Click New.

3. On the SAML Single Sign-On Setting window, complete the following fields, and then click Save.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter the name that will appear when setting up an identity provider. For example: SAS.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuer</td>
<td>This is often referred to as the entity ID for the identity provider. Copy the URL that appears under Subject Alternative Name. For example: <a href="https://idp1.cryptocard.com/idp/shibboleth">https://idp1.cryptocard.com/idp/shibboleth</a></td>
</tr>
<tr>
<td>Identity Provider Certificate</td>
<td>Click Choose File, and then browse to the location where you have downloaded the SAS certificate. (Refer to “Error! Reference source not found.” on page Error! Bookmark not defined..)</td>
</tr>
<tr>
<td>Identity Provider Login URL</td>
<td>Copy the Identity Provider HTTP-POST login URL from SAS, and then paste it here. (Refer to “Error! Reference source not found.” on page Error! Bookmark not defined..) For example: <a href="https://idp1.cryptocard.com/idp/profile/SAML2/POST/SSO">https://idp1.cryptocard.com/idp/profile/SAML2/POST/SSO</a></td>
</tr>
<tr>
<td>Identity Provider Logout URL</td>
<td>Copy the Identity Provider logout URL from SAS, and then paste it here. (Refer to “Error! Reference source not found.” on page Error! Bookmark not defined..) For example: <a href="https://idp1.cryptocard.com/idp/signout.jsp">https://idp1.cryptocard.com/idp/signout.jsp</a></td>
</tr>
<tr>
<td>Service Provider Initiated Request Binding</td>
<td>Select HTTP POST.</td>
</tr>
<tr>
<td>Entity ID</td>
<td>Enter the unique SFDC developer’s domain URL. For example: safenetdemo-dev-ed.my.salesforce.com.</td>
</tr>
</tbody>
</table>
4. On the **SAML Single Sign-On Setting** window, click **Download Metadata**, and then save it to a convenient location.

(The screen image above is from Salesforce®. Trademarks are the property of their respective owners.)
Creating Users in Salesforce

NOTE: A user’s username must be unique across all Salesforce organizations. It must use the format of an email address, but it does not have to be a legitimate email address.

A user’s actual email address can be the same across organizations.

1. On the Salesforce Setup home page, in the left pane, select Administer > Manage Users > Users.

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

2. On the All Users window, click New User.

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

3. On the New User window, complete the following fields, and then click Save:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>Enter the user’s first name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>Enter the user’s last name.</td>
</tr>
<tr>
<td>Alias</td>
<td>Enter the user’s alias.</td>
</tr>
<tr>
<td>Email</td>
<td>Enter the user’s email address. This address must match the address in the E-mail field in SAS. (Refer to the screen shot in “Error! Reference source not found.” in step 4 page Error! Bookmark not defined.)</td>
</tr>
<tr>
<td>Username</td>
<td>The username is automatically displayed.</td>
</tr>
<tr>
<td>Nickname</td>
<td>The nickname is automatically displayed.</td>
</tr>
</tbody>
</table>
Configuring SafeNet Authentication Service

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

- Synchronizing Users Stores to SafeNet Authentication Service, page 12
- Assigning an Authenticator in SafeNet Authentication Service, page 13
- Adding Salesforce as a Service Provider (SP) in SafeNet Authentication Service, page 13
- Enabling SAML Services in SafeNet Authentication Service, page 16

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 Salesforce.

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" 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 Salesforce 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 Salesforce. In this procedure, you will need the metadata that you downloaded in step 4 in “Setting Single Sign-On for Salesforce.”

**To add Salesforce as a Service Provider in** SafeNet Authentication Service:

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. Under **Add SAML 2.0 Settings**, complete the following fields:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>SAML 2.0 Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select <strong>Upload Existing Metadata File</strong>. Click <strong>Choose File</strong> to select the service provider’s metadata file (this is the metadata file that you downloaded in step 4 in “Setting Single Sign-On for Salesforce”), and then click <strong>Open</strong>.</td>
</tr>
</tbody>
</table>

Under **Return Attributes**, add the following attributes, and then click **Apply**:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/claims/EmailAddress">http://schemas.xmlsoap.org/claims/EmailAddress</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
</tbody>
</table>
Enabling SAML Services in SafeNet Authentication Service

After Salesforce 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 SafeNet Authentication Service console with an Operator account.

![Image]

2. Click the ASSIGNMENT tab, and then search for the required user.

![Image]

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 Salesforce 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 Salesforce in the response.
   
c. Click **Add**.
The user can now authenticate to Salesforce using SAML authentication.

### 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 console with an Operator account.

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**:

<table>
<thead>
<tr>
<th><strong>Rule Name</strong></th>
<th>Enter a name for the rule.</th>
</tr>
</thead>
<tbody>
<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 <strong>Virtual Server groups</strong> 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 <strong>Used by rule</strong> box.</td>
</tr>
<tr>
<td><strong>Parties</strong></td>
<td>The <strong>Relying Parties</strong> window lists all service providers. Click the service providers that the groups of users will authenticate to, and then click the right arrow to move the service providers to the <strong>Rule Parties</strong> window.</td>
</tr>
<tr>
<td><strong>SAML Login ID</strong></td>
<td>Select <strong>Email</strong>. The email will be returned to the service provider in the SAML assertion.</td>
</tr>
</tbody>
</table>
Running the Solution

Check the configured solution after successfully configuring the Salesforce for SAML Authentication.

1. Open a web browser and enter the domain URL that you received from Salesforce. In this solution, the following domain URL is used for this integration:

   https://safenetdemo-dev-ed.my.salesforce.com/

   The user is redirected to the SafeNet Authentication Service login page.
2. In the **User Name** field, enter the username, and in the **Password** field, enter the OTP for your enrolled token.

3. Click **Login**.

4. After successful user authentication with SAS, the user is logged into his Salesforce account.

(The screen image above is from Salesforce®. 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>