All information herein is either public information or is the property of and owned solely by Gemalto 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:** 007-012402-002, Rev. E

**Release Date:** June 2016
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicability</td>
<td>4</td>
</tr>
<tr>
<td>Purpose of this Guide</td>
<td>4</td>
</tr>
<tr>
<td>Audience</td>
<td>4</td>
</tr>
<tr>
<td>Terminology</td>
<td>5</td>
</tr>
<tr>
<td>SafeNet Authentication Service Self-Service</td>
<td>5</td>
</tr>
<tr>
<td>Self-Service WSDL API</td>
<td>6</td>
</tr>
<tr>
<td>Overview</td>
<td>6</td>
</tr>
<tr>
<td>Self-Service Site</td>
<td>7</td>
</tr>
<tr>
<td>Self-Service Site Appearance</td>
<td>8</td>
</tr>
<tr>
<td>Inheritance</td>
<td>9</td>
</tr>
<tr>
<td>Module Configuration</td>
<td>9</td>
</tr>
<tr>
<td>Languages</td>
<td>9</td>
</tr>
<tr>
<td>Authorities</td>
<td>10</td>
</tr>
<tr>
<td>Workflow</td>
<td>10</td>
</tr>
<tr>
<td>Provisioning Tasks</td>
<td>10</td>
</tr>
<tr>
<td>Reporting</td>
<td>11</td>
</tr>
<tr>
<td>Configuring the Self-Service Module</td>
<td>11</td>
</tr>
<tr>
<td>Self-Service Policy Module</td>
<td>12</td>
</tr>
<tr>
<td>Set Customization Inherit</td>
<td>12</td>
</tr>
<tr>
<td>Configure Self-Service Appearance</td>
<td>12</td>
</tr>
<tr>
<td>Configure Self-Service Buttons</td>
<td>14</td>
</tr>
<tr>
<td>Configure Self-Service Fonts</td>
<td>15</td>
</tr>
<tr>
<td>Configure Self-Service Modules</td>
<td>16</td>
</tr>
<tr>
<td>Default Elements Module</td>
<td>19</td>
</tr>
<tr>
<td>Request a Token Module</td>
<td>20</td>
</tr>
<tr>
<td>Reset PIP Module</td>
<td>26</td>
</tr>
<tr>
<td>Reset PIP Module</td>
<td>28</td>
</tr>
<tr>
<td>Resync Token Module</td>
<td>30</td>
</tr>
<tr>
<td>Sign In Module</td>
<td>32</td>
</tr>
<tr>
<td>My Profile Module</td>
<td>35</td>
</tr>
<tr>
<td>Configure Self-Enrollment Pages</td>
<td>39</td>
</tr>
<tr>
<td>Self-Service Authorities Module</td>
<td>43</td>
</tr>
<tr>
<td>Request and Approval Queue Processing</td>
<td>45</td>
</tr>
<tr>
<td>Language</td>
<td>46</td>
</tr>
<tr>
<td>Queue Management Module</td>
<td>47</td>
</tr>
<tr>
<td>Reporting</td>
<td>49</td>
</tr>
<tr>
<td>Token Requests Report</td>
<td>49</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>50</td>
</tr>
</tbody>
</table>
Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—A cloud service of SafeNet, Inc.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—The software used to build an authentication service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A term used to describe the implementation of PCE/SPE.

Purpose of this Guide

This guide describes the self-service functionality of the SafeNet Authentication Service platforms. It describes all of the processes required to:

- Customize the Self-Service site
- Automate workflow related to fulfilling user requests for tokens/authentication methods
- Generate, schedule, and automatically deliver relevant reports to workflow and security stakeholders

Users are encouraged to read this guide in the order in which information is presented as successive chapters often rely on information and concepts presented in prior chapters.

Audience

This guide is intended for SafeNet Authentication Service administrators responsible for how managed authentication services are delivered to accounts, and for configuring SAS to reflect the Service Provider’s internal business processes, Service Level Agreements, and management hierarchy.
Terminology

Several terms and their meaning are important to understanding the information presented in this guide:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SafeNet Authentication Service Platforms</td>
<td>This term refers to the capability of the application software used in the SafeNet’s Cloud service, Service Provider Edition used by service providers to delivery their own cloud authentication service and by Enterprises for SPE/PCE requirements for internal use and/or extension to enterprises and individuals with whom they interact (Private Cloud).</td>
</tr>
<tr>
<td>Virtual Server</td>
<td>This term refers to an individual Enterprise’s authentication service delivered by SafeNet Authentication Service (Cloud).</td>
</tr>
<tr>
<td>Subscriber</td>
<td>When presented in all lowercase, the term “subscriber” applies to all accounts that you create and manage. When presented with initial caps, the term “Subscriber” refers to accounts that are not Service Providers.</td>
</tr>
<tr>
<td>Service Providers</td>
<td>These are accounts that, in addition to having their own Virtual Server, are able to create and manage additional accounts.</td>
</tr>
<tr>
<td>Virtual Service Providers</td>
<td>These are service provider accounts that have a service provider as a parent.</td>
</tr>
</tbody>
</table>

SafeNet Authentication Service Self-Service

The SafeNet Authentication Service Self-Service site has been created for organizations that want to:

- Empower users to perform simple authentication management functions, such as resetting PINs and viewing authentication history, which helps to reduce the workload and user reliance on the help desk.

  **NOTE:** To report a lost token, users must contact their administrator or help desk.

- Invite users to request a token. This is particularly useful for organizations servicing consumers of online subscription services. Users can now request a token as part of their subscription for other services.
- Create a customized yet automated workflow for approving token requests, and fulfilling and shipping tokens to users.
- Offer a complete user-centric service, including multi-language support, customized prompts, messages, help, and navigation—all optimized for the user based on how they are interacting with self-service (browser type, screen resolution etc.).
Self-Service WSDL API

Self-service functionality is exposed by the SafeNet Authentication Service platform as a web service (WSDL), giving developers the tools necessary to build some or all of the self-service functionality into a corporate portal. For more information about the self-service WSDL, contact SafeNet or your local vendor.

Overview

Typically, authentication self-service has been limited to extending some token management functionality to “users”; specifically, PIN management, OTP resend, and token resync. The focus is almost always “token-centric”, assuming that all users are the same, have tokens, and that the only issues self-service need resolve are token-related.

In fact, many enterprises want to extend self-service functionality to people that:

- May or may not have tokens. In many organizations, the idea that users should be able to request a token (and/or services) makes sense, perhaps as part of some other service to which the user is subscribing. The concept then is “pull”.
- May or may not be known to the organization. Commonly, users belong to an organization. But this is not always the case. At a simple level, external parties, such as contractors or business partners, may require the service. The separation between the enterprise and the possible user community may broaden. Think of a user becoming a subscriber to your service for the first time. Until they sign up and are approved, the user is completely unknown. Therefore, self-service must accommodate communities that may become legitimate users of the service but are unknown to the service provider prior to “signing-up.”
- May have very diverse requirements, not the least of which is language. It’s difficult to contemplate providing a “global” self-service capability without considering the diversity of the community. It is very unlikely that users will all speak the same language or that hardware tokens shipped from Toronto will arrive in Montreal and Shanghai in the same timeframe. In other words, self-service needs to accommodate diversity in such a way as to maximize the simplicity of the user experience, regardless of language, logistics, and authentication method.

It is quickly apparent that the “pull” world demands a new set of tools by which administrators of authentication services can extend self-service functions to current and potential users, determine the validity of requests, how each is to be handled and how, throughout the process, the user is kept informed.

The key elements to producing an effective and highly marketable self-service capability depend on:

- Ensuring that the approval process reflects the enterprise’s desired workflow
- Sufficient visibility at all stages of the workflow as to the status of a request
- Effective and simple workflow and communication with the user

All self-service functionality, from what is presented to the user to back-office workflow, is controlled through the configuration and management modules contained on the Self-Service tab of the SafeNet Authentication Service platform.
Self-service then is best viewed as three functional areas:

- The Self-Service website, through which users perform common functions.
- Presentation services, through which administrators customize the services, languages, and other aspects of self-service presented to users on the Self-Service site.
- Back-end workflow, through which administrators manage the services presented to users through the Self-Service website.

**Self-Service Site**

All configuration and management of self-service is performed in SAS from the Self-Service tab of a virtual server. The following functions are available on this tab:

- **Configure Self-service Module**—The links in this module provide access to all of the functions related to customizing the site for appearance, user services, and back-office workflow, including approving and fulfilling user requests for tokens.
- **Queue Management Module**—This module provides lists of outstanding tasks related to user requests for tokens. Operators with appropriate “authorities” can view and process requests for tokens.

![Figure 1: Self-Service Tab](image-url)
The **Self-Service** site can present users with the following modules:

<table>
<thead>
<tr>
<th>Service</th>
<th>Default Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Request a Token</strong></td>
<td>![Token Icon]</td>
</tr>
<tr>
<td>This service allows users to request a token by type from a list of approved token types and authentication methods. This service accommodates both existing users, as well as creation of new user accounts. This module is not published by default.</td>
<td></td>
</tr>
<tr>
<td><strong>Reset PIN</strong></td>
<td>![PIN Icon]</td>
</tr>
<tr>
<td>This module allows users to modify their server-side PIN without the assistance of the help desk. PIN changes must comply with the PIN policy. This module is published by default.</td>
<td></td>
</tr>
<tr>
<td><strong>Reset PIP</strong></td>
<td>![PIP Icon]</td>
</tr>
<tr>
<td>This module allows users to modify the PIP (personal identification pattern) associated with their GrID authentication method without the assistance of the help desk. The new PIP must comply with the PIP policy. This module is published by default.</td>
<td></td>
</tr>
<tr>
<td><strong>Resync Token</strong></td>
<td>![Token Icon]</td>
</tr>
<tr>
<td>This module allows users to test and resync their token with the server without the assistance of the help desk. This module is published by default.</td>
<td></td>
</tr>
<tr>
<td><strong>My Profile</strong></td>
<td>![Profile Icon]</td>
</tr>
<tr>
<td>This module can allow users to modify basic information about their account such as address, telephone number, etc. It also presents basic statistics about their authentication activity and allows them to manage challenge/response questions valid (if enabled) for sign-on to the Self-Service site. This module is not published by default.</td>
<td></td>
</tr>
<tr>
<td><strong>Resend SMS</strong></td>
<td>![SMS Icon]</td>
</tr>
<tr>
<td>This module allows a user to request an SMS/OTP resend to their registered mobile device.</td>
<td></td>
</tr>
</tbody>
</table>

**Self-Service Site Appearance**

The **Self-Service** site is highly customizable within each virtual server. This includes:

- Navigation and other buttons
- Logos and icons
- Fonts
- Colors
Inheritance

By default, when a Subscriber account is on-boarded, (for example, a child account created by the Service Provider), it inherits all customizations applied to the Service Provider’s Self-Service site. Subscriber accounts can override these customizations and independently configure their Self-Service site.

![Figure 2: Self-Service Site Inheritance](image)

To override default or Service Provider customizations, select the **Set Customizations Inherit** link, clear the **User Inherit Customizations** option, and then click the **Apply** button. To revert to default site settings which do not inherit from the Service Provider customizations, select the option and then click **Apply** to commit the change.

Module Configuration

Each module is enabled and configured independently for user options and supported languages. Modules may contain more than one web page to be presented to the user.

![Figure 3: Module Configuration](image)

Languages

The Self-Service site can be configured to provide services in any number of languages. The default service is based on an English language set. Administrators can create additional language sets using the English set as a guide.
Authorities

Authorities are special privileges assigned to Operators for the purpose of managing user requests for tokens received from the Self-Service site. There are four possible Authorities:

- **Approval Level 1**—This Authority approves or denies user requests for tokens received from the Self-Service site. At least one Operator must have this Authority if the Request a Token module is enabled on the Self-Service site.

- **Approval Level 2**—This Authority approves or denies user requests for tokens that have been approved by Approval Level 1 authorities. This is an optional Authority.

- **Issuing Authority**—Requests for tokens that have received the required approvals are fulfilled by the Issuing Authority. This function is the equivalent of using the Provision functions available on the Assignment tab unless a Shipping Authority has been created. At least one Operator must have this authority if the Request a Token module is enabled on the Self-Service site.

- **Shipping Authority**—The Shipping Authority is a special function that serves two purposes:
  
  - It can be used to coordinate the delivery of enrollment instructions with receipt of the physical token by the user.
  
  - It can be used to increase the security of enrollment by requiring the user to provide an additional code during enrollment that is delivered separately and out-of-band (“OOB”) with respect to all other enrollment instructions.

  Shipping authorities are applied by token type. Token requests for affected token types that have been approved by the Issuing Authority must be completed by the Shipping Authority. This is an optional authority.

Workflow

Requests for tokens include workflow that incorporates appropriate messaging and alerts for the users making requests for tokens and for each Authority involved in the approval and fulfillment process. Alerts and messages can be customized and sent by email and/or SMS. In addition, all requests can be viewed and managed from the Queue Management module.

Provisioning Tasks

A provisioning task is created for each fulfillment. Tasks can be viewed by clicking the Provisioning Tasks link in the Shortcuts section on the Assignment tab. A provisioning task shows the date the enrollment reservation was created, the date by which enrollment must be completed, and the status of the enrollment. Tasks may be cancelled or modified prior to user enrollment, and an alert can be generated for expired enrollments. For more information on provisioning tasks, refer to the SAS Service Provider Administrator Guide.
Reporting

All self-service requests for tokens and subsequent processing by authorities are available in reports (Reports tab) including:

- **Provisioning Task Attempts**—Reports details of attempts to use provisioning tasks by users.
- **Provisioning Tasks**—Reports details of provisioning tasks.
- **Provisioning Tasks – Outstanding**—Lists all outstanding provisioning tasks

Configuring the Self-Service Module

In this module:

- **Self-Service Policy**—Use this module to view or modify the Self-Service site’s unique URL.
- **Set Customization Inherit**—Use this module to override site customizations inherited from the Service Provider or to revert to default settings.
- **Configure Self-Service Appearance**—Use this module to configure the overall site “look and feel”, including colors, logos, and banner images.
- **Configure Self-Service Buttons**—Use this module to modify navigation items, such as buttons, button text, and module icons.
- **Configure Self-Service Fonts**—Use this module to select font types and styles used throughout the site.
- **Configure Self-Service Modules**—Use this module to customize each of the modules published to the Self-Service site, including language sets, required/optional fields, and user help and instructions.
- **Configure Self-Service Enrollment Pages**—Use this module to customize instructions presented to the user during token enrollment. Instructions and messages can be created independently for each token type.
- **Self-Service Authorities**—Use this module to add one or more Authorities to Operators.
- **Out-of-Band Enrollment**—Use this module to require the use of an additional factor during enrollment, delivered to the user “out of band”.
- **Request and Approval Queue Processing**—Use this module to customize message content and delivery method provided to users that have requested a token and to Authorities.
- **Language**—Use this module to select the Self-Service default language.
Self-Service Policy Module

This module displays the base URL and unique URL for the Self-Service site. The **Self-Service Unique URL** must be provided to users. These URLs are automatically created when the virtual server account is activated. These URLs should not be modified unless a stand-alone Self-Service site has been installed and configured, in which case these URLs should reflect the location of that web server.

<table>
<thead>
<tr>
<th>Self Service Policy:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apply</strong></td>
</tr>
</tbody>
</table>

**Figure 4: Self-Service Policy**

Set Customization Inherit

Use this module to override site customizations inherited from the Service Provider or to revert to default settings. To customize the site, clear the **Use Inherit Customizations** option, and then click **Apply** to commit the change.

<table>
<thead>
<tr>
<th>Set Customization Inherit:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apply</strong></td>
</tr>
<tr>
<td>Use Inherit Customizations:</td>
</tr>
</tbody>
</table>

**Figure 5: Set Customization Inherit**

Configure Self-Service Appearance

Use this module to change the colors and logos used in the Self-Service site:

- **Self-Service Logo**—This is the logo that will appear near the top center of Self-Service site. Uploaded logos should be in png, jpg, or gif format, and 387 x 70px.
- **Logo Background Color**—This is the color behind the logo and spans the width of the page. Dimensions: page width x 70px.
- **Banner Image**—This is an image in the banner area, which includes the navigation buttons. Dimensions: page width x 80px.
- **Banner Color**—This is the color behind the banner image and spans the width of the page. Dimensions: page width x 80px.
- **Homepage Background**—This is the image used on the home page background. Dimensions: page width x 80px (max).
- **Homepage Color**—This is the home page background color displayed behind the Homepage Background image.
- **Page Background**—This is the background image used on all pages other than the home page.
- **Page Color**—This is the page background color displayed behind the Page Background image on all pages other than the home page.
- **Language Icon**—This is an optional icon displayed in the page footer to represent language selection options on the page.
- **Help Text Background**—This is the background color of all available help text available on the site.
- **Error Text Background**—This is the background color behind all error messages.
- **Input Field Border Color**—This is the color of the border surrounding input fields.
- **Input Field Background Color**—This is the color of the input fields.

![Figure 6: Configure Self-Service Appearance](image-url)
Configure Self-Service Buttons

Use this module to change the buttons and icons used in the Self-Service site:

- **Small Button**—These are the buttons used for navigation throughout the site. Button images can be uploaded, selected from a list of available buttons, or configured as an HTML button. Uploaded buttons should be dimensions 120 x 28px.

- **Button Text**—This provides options to select the font, font size, color, and weight used on small buttons.

- **Button Hover Text**—This provides options for modifying the appearance of the button text when hovering over the button.

- **Large Button**—Some selection options, such as choosing the type of token, use a large button. Button images can be uploaded, selected from a list of available buttons, or configured as an HTML button. Uploaded buttons should be dimensions 400 x 28px.

- **Icons**—Module icons can be replaced with uploaded images. Icons should be in png, jpg, or gif format and be 100 x 100px.

- **Language Icon**—The language icon can be replaced with an image or text. Images should be 96 x 20px.

![Configure Self-Service Buttons](image)

**Figure 7: Configure Self-Service Buttons**
Configure Self-Service Fonts

Use this module to change the fonts icons used in the Self-Service portal where:

- **Site Title**—This is the site title displayed in the banner area.
- **Page Title**—This is the title below the banner area and to the left of the | separator.
- **Page Service**—This is the title below the banner area and to the right of the | separator.
- **Field Label**—This is the font used throughout the site for all field labels.
- **Help Text**—This is the font used in all help panels.
- **Error Text**—This is the font used for all error messages.
- **Footer Text**—This is the font used in the footer area of the site.

![Configure Self-Service Fonts](image)

**Figure 8: Configure Self-Service Fonts**
Configure Self-Service Modules

Use this module to configure Self-Service modules.

Language Set

This area supports the viewing and creation of multiple language sets for each of the Self-Service modules, and all of the pages, error messages and help text available in each module.

Figure 9: Configure Self-Service Modules

To view a language set, select it from the language list, and then click the View button.

To add a language set, type the name for the set in the Language set field, and then click the Add button. Next, modify all of the labels, default text, help text, and error messages for each of the pages in the selected module. For example, to create a French language set:

1. Add French to the list.
2. Select a module from the **Module** list.

3. Select a page from the **Pages** list, and then modify the text and labels.

4. Click **Apply** to save the set. Repeat steps 3 and 4 until all pages have been modified.
Self-Service Module Options

A module is published to the Self-Service site if it is enabled. Referring to Figure 10: Self-Service Module Options:

- **Enable Module Option – Highlighted Area 1**—To change the publication status of a module, select or clear the Enable option and then click Apply.

- **Require the User to Sign in – Highlighted Area 2**—For security reasons, some modules, such as My Profile or Change PIN, should require the user to authenticate before access is granted. To require authentication, select this option and then click Apply.

- **Use Page – Highlighted Area 3**—Most modules contain several pages; however depending on your requirements, it may not be necessary to publish all pages. For example, the My Profile module includes pages that display token requests made by the user. As this is an information page only, it is not necessary to publish the page.

- **Show Help – Highlighted Area 4**—Help is available for most pages; however, it can be removed from the site by clearing this option.

- **Required – (not shown)**—Some pages, such as My Profile, allow users to input or update information. The Required option, if enabled, requires the user to enter data into the field. If this option is not selected, the field is not displayed.

![Figure 10: Self-Service Module Options](image-url)
Default Elements Module

This module has only one page and includes the basic information presented on the Self-Service site home page. User access to customized Terms of Use policies and documentation can be provided by placing these on a publicly accessible location and updating the corresponding URLs in this module.

The **Language** icon can be replaced with text or a custom image (refer to “Configure Self-Service Buttons” on page 14).

The **Help Desk** link in the footer area should contain information that assists the user in contacting your help desk for assistance.

**Figure 11: Default Elements Module**
Request a Token Module

This module provides the ability for a user to request a token. It is also where outbound messages to users and authorities are configured. To make this module available on the Self-Service site, the following must be in place:

- The virtual server must have at least one Operator.
- The **Enable Request a Token** option must be enabled here and under the **Self-Service Authorities** module. Although both options must be enabled in order for the **Request a Token** button to be available on the Self-Service site, enabling the option here (under the **Request a Token** module) allows you to show or hide the **Request a Token** button on the home page on the Self-Service site; however, it has no effect on the function itself, which will continue to run while the same option is enabled under **Configuring Self-Service > Self-Service Authorities**. Hiding the button simply prevents users from requesting new tokens, allowing administrators time to process existing requests that are currently in the token request queue.

![Request a Token Page](image)

**Figure 12: Request a Token Page**

There are six (6) pages in this module:

- User Type Page – page 21
- Create Account Page – page 21
- Token Type Page – page 22
- Confirmation Page – page 23
- Validation Page – page 23
- User Page – page 24
User Type Page

This is the first page presented to the user when accessing this module. Users that have an account and an assigned authentication method, such as a token, can sign in to the Self-Service site and request an additional token.

This page also allows users that do not have an account in the virtual server to create an account (pending approval) as part of the token request process.

Create Account Page

If enabled, the user will be able to submit a request to create an account in the virtual server during the “request a token” process. The request must be approved by Approval Level 1 (and Approval Level 2 if enabled) before the account is created.

The fields **First Name**, **Last Name**, **User ID**, and **E-mail address** are mandatory if this page is enabled. Other fields can be displayed by selecting the corresponding **Required** option.

To unpublish (hide) the **Create Account** page, clear the **Use Page** option.
**Token Type Page**

This page displays a list of token types that may be requested by the user. Each type in the list has a corresponding enrollment class. For example, the MP for iPhone/iPad would use the **Software** enrollment class. The class selection determines which notification and enrollment instructions the user will receive for the selected token type.

![Token Type Page](image)

**Figure 15: Request a Token - Token Type Page**

To publish or unpublish a token type, select or clear the corresponding field option respectively, and then click **Apply**.

**To add a token type:**

1. Click the **Add Token Type** button.
2. Enter a description and select a class from the list.
3. Select the **Field** option.
4. Click **Apply**.
Confirmation Page

The **Confirmation** page is used to configure messages that will be displayed to the user immediately following token selection.

![Confirmation Page](image1)

**Figure 16: Request a Token - Confirmation Page**

Only one of the messages will be displayed, corresponding to the type of validation required/available.

Validation Page

The **Validation** page is used to configure messages that will be displayed to the user for token validation. If enabled, the user must confirm their request for a token by replying to a message delivered to them via email and/or SMS. To enable or disable the validation requirement, select or clear the **Use Page** option and then click the **Apply** button.

![Validation Page](image2)

**Figure 17: Request a Token - Validation Page**
User Page

This page is displayed when the user selects the I am an Existing User option. It requires the user to provide their User ID when signing in to the Self-Service site.

- **User ID**: The label for the User ID input field.
- **Error**: The error message displayed if the User ID is not valid.
- **Next**: Text for the Next button.

![Figure 18: Request a Token - User Page](image)

SafeNet Authentication Service (SAS): Self-Service Administrator Guide
Document PN: 007-012402-002, Rev. E
Figure 19: Request a Token Workflow
Reset PIN Module

This module provides the ability for a user to reset the server-side PIN associated with a token assigned to them. There are five (5) pages in this module. Each module contains a section for error messages and/or help text.

User Page

This is the content of the first page served to the user when accessing the Reset PIN facilities. If the page is set to require the user to sign in, they will be directed to the Sign In page before being presented with the User page.

Select a Token Page

If a user has more than one token, this page provides a list from which the user can select the token. PIN reset applies to the selected token.
Create New PIN Page

This page is presented when the user has supplied their UserID and the serial number of a token assigned to their account and the PIN associated with the token allows the user to generate a new PIN (for example, server-side, user select). It requires the user to enter and verify a new PIN.

Figure 22: Reset PIN - Create New PIN Page

Server-Side PIN Page

This page is displayed if the token issued to a user requires a server-side PIN that is set by the server (for example, server-side, server select).

Figure 23: Reset PIN - Server Side PIN Page
Confirmation Page

This page is presented when the user has successfully changed their PIN.

Reset PIP Module

This module provides the ability for a user to reset the PIN associated with their GrID authentication method. There are three (3) pages in this module. Each module contains a section for error messages and/or help text.

User Page

This is the content of the first page served to the user when accessing the Reset PIP facilities. If the page is set to require the user to sign in, they will be directed to the Sign In page before being presented with the User Page.

If directed to sign in, the user should only provide their UserID. If an OTP field is displayed on the sign in page, it should be left blank. A valid userID and empty OTP field will generate a new page with a GrID and OTP field, allowing the user to authenticate and sign in.
Select Pattern Page

This page is presented for a valid UserID provided on the User page and requires the user to authenticate using their current PIP.

Figure 26: Reset PIP - Select Pattern Page

Confirmation Page

The confirmation page is presented on successfully resetting a PIP.

Figure 27: Reset PIN - Confirmation Page
Resync Token Module

This module provides the ability to resync a token with the server and confirm the ability to authenticate with the token. There are six (6) pages in this module. Each module contains a section for error messages and/or help text.

User Page

The user page is served up to the user in two parts—the first requires the UserID, which, if found on the server, generates the second part requesting the token serial number.

![Resync Token - User Page](image)

Figure 28: Resync Token - User Page

Auth Resync Page

This page is presented when the selected token supports resynchronization using two consecutive OTPs.

![Resync Token - Auth Resync Page](image)

Figure 29: Resync Token - Auth Resync Page
Time-based Resync Page

This page is presented when the selected token is time-synchronous and supports resynchronization using two consecutive OTPs.

![Time-based Resync Page](image)

**Figure 30: Resync Token – Time-based Resync Page**

Challenge/Response Page

The challenge/response page is presented when a token fails resynchronization using all other available methods. In this method the user must key the displayed challenge into their token to generate a passcode or “response”, and then enter the response in the indicated field.

![Challenge/Response Page](image)

**Figure 31: Resync Token - Challenge/Response Page**
Confirmation Page

The confirmation page displays the outcome of the synchronization attempt whether successful (Confirmation), failed (Error) or not processed (No Token Error).

![Confirmation Page Image]

Figure 32: Resync Token - Confirmation Page

Sign In Module

This module provides controls the options for signing into the self-service site. There are five (5) pages in this module. Each module contains a section for error messages and/or help text. The Sign In button is replaced with a Sign Out button when a user successfully authenticates to the Self-Service site.

Authenticate Page

This page presents the allowed methods for authenticating into the Self-Service site. The remaining pages in this module provide the user experience and process necessary for the method selected by the user.

![Authenticate Page Image]

Figure 33: Sign In - Authenticate Page
Authenticate to Process Page

This page handles authentication using tokens, grids and static passwords. It includes additional prompts to deal with authentication exceptions. In most cases a user authenticating using a token will provide their OTP and gain access to the site. However, it is possible that another policy will be triggered altering this workflow.

For example, if there is a server policy that requires the user to change their PIN every 30 days and this happens to coincide with their authenticating to the self-service site, successful authentication will be followed with a requirement to create a new PIN before access to self-service is permitted. This page provides prompts that deal with such situations.

Figure 34: Sign In - Authenticate to Process Page

Send Password by E-mail Page

This selection sends a one-time password, valid only for the Self-Service site to the email address associated with the userID. It includes error messages to handle cases where email cannot be sent or the userID cannot be found.

Figure 35: Sign In - Send Password by Email Page
Send Password by SMS Page

This selection sends a one-time password, valid only for the self-service site to the SMS number associated with the userID. It includes error messages to handle cases where SMS cannot be sent or the userID cannot be found.

![Sign In | Send Password by SMS](image)

**Figure 36: Sign In - Send Password by SMS Page**

Sign in using Questions and Answers

This option allows a user to sign in using answers to questions provided when configuring their profile.

![Sign In | Authenticate](image)

**Figure 37: Sign In using Questions and Answers**
My Profile Module

This module can allow users to modify basic information about their account such as address, telephone number etc. It also presents basic statistics about their authentication activity and allows them to manage challenge/response questions valid (if enabled) for sign on to the Self-Service site. There are five (5) pages in this module. Each module contains a section for error messages and/or help text.

This module requires sign in to the self-service site.

Select to Proceed Page

This is the first page displayed when My Profile is selected by the user.

View my Logon Statistics

This displays information about authentication activity by the user including last logon date, number of logons: today, this week this month and this year. This page can be unpublished.

Figure 38: My Profile Module - Select to Proceed Page

Figure 39: View my logon statistics
View and Update my Profile

The user can update basic personal information that is stored in the virtual server. Note that this module cannot be used to update information obtained by the virtual server from an external user source such as LDAP. Only users that have been manually created or imported from a flat file can update their information through this module.

This module lists the fields that will accept user input. Some are mandatory (no options), others can be required (made mandatory). It also contains sections for customizing error messages and adding help text relevant to this page.

![View and update my profile](image)

Figure 40: View and update my profile

Update my Security Questions and Answers

Security Questions and Answers can be used as an alternative sign-in method for the self-service site. This module allows the administrator to create a series of questions. The user will be required to create a set of answers to these questions. During sign-in the user will have the option of supplying the previously recorded answers to the questions as an alternative sign-in method if this method is enabled. This page can be unpublished.

![Update my security Questions and Answers](image)

Figure 41: Update my security Questions and Answers
**Question Management Page**

Use this page to create questions from which the user will select as an alternate self-service site sign in method.

![Question Management Page](image)

**Figure 42: My Profile Module | Update my security questions and answers | Question Management**

In this module:

- **Question Management Dropdown**
  This dropdown provide access to three pages used to configure security question and answers:

- **Question Management**
  Use this page to create questions.

  Use the **Edit** button to modify a highlighted question from the defined question list, including the minimum and maximum answer length, case sensitivity and trivial answer control options.

  Use the **Add** button to add a question created in the **Question** field to the **Defined Questions** list.

**Question Sets Page**

Use this page to define the number of question groups that will be displayed to the user. Users must answer one question from the list of questions contained in a Question Set.

![Question Sets Page](image)

**Figure 43: My Profile Module | Update my security questions and answers | Question Sets**

Use the arrows to add or remove question sets to or from the **Defined Question Sets** list. Sets in this list are displayed to the user.
**Question Assignment**

Use this page to group questions created in **Question Management** into one or more of the sets enabled in **Question Sets**.

![Figure 44: My Profile Module | Update my security questions and answers | Question Assignment](image)

To add one or more questions to a set, select the set from the dropdown list, then using the arrows move the questions to be included in the set to the **Questions in Sets** list, then click the Update button to commit the change.

- **Minimum answer length**
  Sets the minimum number of characters allowed as an answer.

- **Maximum answer length**
  Sets the maximum number of characters allowed as an answer.

- **Answers are case sensitive**
  If checked, answers are case sensitive.

- **Disallow trivial answers**
  If checked, answers comprised of triplets (for example, 111, aaa) or 3 character sequential strings (for example, 123, abc) are disallowed.

Use the **Add** button to add questions to the list. To edit or remove a question, highlight it in the list then click the **Edit** or **Remove** button respectively.

**My Token Request**

This page displays a list of outstanding token requests.
Configure Self-Enrollment Pages

Self-enrollment pages are presented to the user allowing enrollment, binding of the token to the user and activation of the token. Different token types and authentication methods require different enrollment steps. This module contains a page for each enrollment process. This module includes the pages described below.

Default/Common Page

This page contains elements that are used in all enrollment processes. The use of these elements varies, depending on the token type and enrollment process. For example, UserID and Activation code may be prompts on an enrollment page, or may be used as labels in enrollment emails/SMS messages.

In any case, these prompts should be translated for each language set to be supported on the Self-Service site.

<table>
<thead>
<tr>
<th>Field</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID :</td>
<td>UserID :</td>
</tr>
<tr>
<td>Activation Code :</td>
<td>Activation Code :</td>
</tr>
<tr>
<td>Clear</td>
<td>Clear</td>
</tr>
<tr>
<td>Next</td>
<td>Next</td>
</tr>
<tr>
<td>E-mail :</td>
<td>E-mail</td>
</tr>
<tr>
<td>Unrecoverable database or web server error :</td>
<td>Unrecoverable database or web server error :</td>
</tr>
<tr>
<td>Authentication failed. Please, try again!</td>
<td>Authentication failed. Please, try again!</td>
</tr>
<tr>
<td>SafeNet Authentication Service</td>
<td>SafeNet Authentication Service Self-Enrollment requires an SSL connection.</td>
</tr>
<tr>
<td>Your token has been successfully activated. Please remember your User ID below.</td>
<td>Your token has been successfully activated. Please remember your User ID below.</td>
</tr>
</tbody>
</table>

Figure 45: Self-Enrollment - Default/Common Page
Software Token Page

This is a very lengthy page which contains all of the prompts, error messages, and instructions for enrolling MP-1 software tokens for each of the possible target devices (iOS, Android, BlackBerry, JAVA, Windows, and OS X).

These prompts and messages should be translated for each language set to be supported on the Self-Service site.

Figure 46: Self-Enrollment - Software Token Page

Custom Token Page

This page contains all of the prompts, error messages, and instructions for enrolling custom tokens.

These prompts and messages should be translated for each language set to be supported on the Self-Service site.

Figure 47: Self-Enrollment - Custom Token Page
Hardware Token Page

This is a very lengthy page which contains all of the prompts, error messages, and instructions for enrolling hardware tokens (RB-1, KT-x, eTokenPASS, RADIUS tokens, and third-party tokens).

These prompts and messages should be translated for each language set to be supported on the Self-Service site.

![Hardware Token Page](image)

Figure 48: Self-Enrollment - Hardware Tokens Page

Password Page

This page contains all of the prompts, error messages, and instructions for enrolling a static password.

These prompts and messages should be translated for each language set to be supported on the Self-Service site.

![Password Page](image)

Figure 49: Self-Enrollment - Password Page
MobilePASS Page

This is a very lengthy page which contains all of the prompts and instructions for enrolling MobilePASS tokens for each of the possible target devices (iOS, Android, BlackBerry, JAVA, Windows, and Mac OS X). Note: QR code enrollment will be available in a future release.

The Multi-Device Instructions section may be useful to:

- Provide assistance to users when the device where the page is loaded is not a selected allowed target. **Allowed Targets Settings** are designed to allow the user to choose the instructions related to his/her chosen device type, and are selected in POLICY > Token Policies, and
- Provide instructions to users who may be loading the Self-Enrollment page on a device that is not their intended device for enrolling the token (and wish to only review the instructions).

The Multi-Device Instructions section will be displayed only if the Enable Multi-Device Instructions check box is selected in POLICY > Automation Policies > Self-Enrollment Policy.

- For new accounts created in SAS v3.5 (and higher), this option is enabled by default.
- For existing customers, after an upgrade to SAS v3.5, this option is disabled by default.

These prompts and messages should be translated for each language set to be supported on the Self-Service site.

![Image of MobilePASS Page]

Figure 50: Self-Enrollment - MobilePASS Page
Self-Service Authorities Module

Authorities are special privileges assigned to Operators for the purpose of managing user requests for tokens received from the Self-service site. There are four possible Authorities:

- **Approval Level 1**—This authority approves or denies user requests for tokens received from the Self-Service site. At least one Operator must have this authority if the Request a Token module is enabled on the Self-Service site.

- **Approval Level 2**—This authority approves or denies user requests for tokens that have been approved by Approval Level 1 authorities. This is an optional authority.

- **Issuing Authority**—Requests for tokens that have received the required approvals are fulfilled by the Issuing Authority. This function is the equivalent of using the Provision functions available on the Assignment tab unless a Shipping Authority has been created. At least one Operator must have this authority if the Request a Token module is enabled on the Self-Service site.

- **Shipping Authority**—The Shipping Authority is a special function that serves two purposes:
  - It can be used to coordinate the delivery of enrollment instructions with receipt of the physical token by the user.
  - It can be used to increase the security of enrollment by requiring the user to provide an additional code during enrollment that is delivered separately and Out-of-Band (OOB) with respect to all other enrollment instructions.

Shipping authorities are applied by token type. Token requests for affected token types that have been approved by the Issuing Authority must be completed by the Shipping Authority. This is an optional authority.

Configuring Authorities

Begin from the Configuring Self-Service module > Self-service Authorities link. This will display a list of Operators that can be assigned one or more authorities. To enable an authority for an Operator, select the appropriate authority option, and then click the Apply button to commit.

There must be at least one Operator with Approver Level 1 Authority and/or Issuing Authority to activate the Enable Request a Token. Unless enabled, the Request a Token option will not appear on the Self-Service site.

Likewise, if a token is in the Shipping Authority Required list, at least one Operator with Shipping Authority is required.

![Figure 51: Configure Self-Service Authorities](image-url)
At least one Approval Level 1 and Issuing Authority must be enabled.

Figure 52: Self-Service Workflow

To add a shipping authority to a token type, first ensure that at least one Operator has been given this authority. Refer to "Configuring Authorities" on page 43. Next, select the token type from the **Not Required** window and, using the arrow, move it to the **Shipping Authority Required** window. Repeat this step for each token type that will require a shipping authority.

**Out-of-Band Notification**

Out-of-band (OOB) notification requires that the user provide an additional factor during enrollment to further validate their identity. This normally is in the form of an activation code. The code can be delivered by email, SMS, or output to a file.

OOB can be used with both hardware and software tokens. To enable OOB, select the tokens to which it will apply and the activation code delivery methods, and then click the **Apply** button.

Figure 53: Out of Band Notification
Request and Approval Queue Processing

This module contains a page for each of the messages that will be sent to the user and each of the authorities during the approval and provisioning processes. The intent is that both users should be kept informed of the status of the request and authorities should be notified when action is required of them.

Each message has an enable/disable option. If enabled, the message is sent at the appropriate point in the process. If disabled, the message is not sent.

Configure Request and Approval Queue Processing

The following configuration options are available in this module:

- **Auto-delete unapproved requests after X days**—If set to 0, unapproved requests will not be automatically removed from the Approval queue. Any other value will automatically remove an unapproved request the indicated number of days after it was received.

- **Allow approval by Email/SMS**—Check the delivery method(s) the system will use to send status and action alerts to authorities. If none are checked, status and action alerts will not be sent but the request will be listed in the appropriate queue.

This module contains several notifications. Use the menu in the Configure Queue Processing section to select the message. Each message has three (3) sections — two (2) for email (Subject, Body) and one (1) for SMS (SMS Content). Most messages contain variables (example: <email />) that must not be removed or modified. Otherwise, modify any other element of each notification according to your needs.

Keep in mind that there is a 160-character limit (including white space) in SMS messages. To prevent a multi-part SMS message, avoid exceeding this limit.

Click **Apply** after each message modification to commit the change.

![Request and Approval Queue Processing](image)

Figure 54: Request and Approval Queue Processing
Language

This module is used to specify the default language for the Self-Service site. The English and French language sets are pre-configured, with English as the default. Additional language sets can be created using any existing language set as a guide. It should be noted that log files will always be presented in the English language.

To specify a language, select it from the **Self-Service Default Language** list and then click **Save**.

![Language Configuration](image)

**Figure 55: Language Configuration**

If a user wishes to set their own personal language preference for the Self-Service site, they can do so on the Self-Service site **Login** page and **Home** page. At the bottom of the page, a text or icon link for languages will be displayed, based on configuration of the Self-Service module (the default links are shown below).

To switch to another language, click the languages link and then select the language from the list. All text in the Self-Service site will be converted to the selected language upon log in for that user only.

<table>
<thead>
<tr>
<th>To change the default user language</th>
<th>Languages text link</th>
<th>Languages icon link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a link on the Self-Service site home page…</td>
<td>Languages</td>
<td><img src="image" alt="Language Icons" /></td>
</tr>
<tr>
<td>…and then select a language.</td>
<td>SELECT A COUNTRY/REGION</td>
<td></td>
</tr>
<tr>
<td></td>
<td>English</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Français</td>
<td></td>
</tr>
</tbody>
</table>
Queue Management Module

The **Queue Management** module provides the interface for each of the authorities to process requests. Use the **State** menu to select the **Authority Queue** to be viewed. Note that an Operator is not able to view a queue for which they do not have the corresponding authority.

Select a **Request State** from the list, and then click **Search** to update the list for the selected state.

All queues have a list containing requests waiting processing. Each row in the list shows:

- **Request ID**—This is a unique number that identifies this request through all of the queues. As soon as a request has been issued, a provisioning task is created using the same ID number. Provisioning tasks track the user’s enrollment activity.
- **Submit Date**—This is the date and time the user submitted the request.
- **User ID**—This is the user ID associated with the request. Click the link to view information about the user. This will correspond with the data for this user ID found under **Assignment > User Detail**.
- **First Name**—This is the user’s first name.
- **Last Name**—This is the user’s surname.
- **Email**—This is the email address associated with this user.
- **Token Type**—This is the token type requested by the user.
- **Process State**—This indicates the state of the request. Currently, the only option is **Pending Approval**.

![Queue Management](image)

**Figure 56: Queue Management**

- **Approval Level 1**—Displays a list of all requests awaiting this approval. Select one or more requests then click **Level 1 Approve** or **Reject**.
  - If the request is approved and Approval Level 2 is enabled, the request will be removed from this list and appear in the Approval Level 2 queue, otherwise it will appear in the Issuer queue.
  - If enabled, the user will receive a “Request Approved” or “Request Rejected” notification corresponding to the Authorities decision. If approved and enabled, the next Authority in the processing sequence will receive a notification.
• **Approval Level 2**—Displays a list of all requests awaiting this approval. Select one or more requests then click Level 2 Approve or Reject to approve or reject the request respectively.
  - If the request is approved the request will be removed from this list and appear in the Issue queue.
  - If approved and enabled, the next Authority in the processing sequence will receive a notification.

• **Issue**—Displays a list of all requests awaiting this approval. Select one or more requests then click Issue Approve or Reject to approve or reject the request respectively.
  - If the request is approved and Shipping Authority is enabled for the requested token type, the request will be removed from this list and appear in the Shipping queue, otherwise the enrollment messages will be sent to the user.
  - If approved, a Provisioning Task will be created. The task tracks the status of the enrollment, including enforcement of enrollment policies such as last date to enroll.

• **Shipping Queue**—Displays a list of all requests awaiting this approval. Select one or more requests then click **Issue Approve** or **Reject** to approve or reject the request respectively.
  - The must receive an out of band activation code/instructions. The method of delivery is determined by the selection by token type.
  - If approved, a Provisioning Task will be created. The task tracks the status of the enrollment, including enforcement of enrollment policies such as last date to enroll. Tasks may be view from the **Assignment > Provisioning Tasks**.
Reporting

Token requests data and related workflow activity is recorded in the database. A number of reports are available to extract this data:

**Token Requests Report**

This report captures all requests and their progress through the workflow including:

- Request ID
- User ID
- First Name (user)
- Last Name (user)
- Email (user)
- Token Type (requested)
- Request State (Approval 1, Approval 2, Issue, Ship)
- Request Date
- Approval Date
- Approved By
- Issued Date
- Issued By
- Shipped Date
- Shipped By

Other relevant reports are the Provisioning Task Attempts, Provisioning Tasks and Provisioning Tasks Outstanding reports. Refer to the *SAS Service Provider Administrator Guide* for additional information.
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>Address</td>
<td>Gemalto&lt;br&gt;4690 Millennium Drive&lt;br&gt;Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td>Phone</td>
<td>US&lt;br&gt;1-800-545-6608&lt;br&gt;International&lt;br&gt;1-410-931-7520</td>
</tr>
<tr>
<td>Technical Support</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Customer Portal</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>