Copyright © 2012 SafeNet, Inc. All rights reserved.

All attempts have been made to make the information in this document complete and accurate.

SafeNet, Inc. is not responsible for any direct or indirect damages or loss of business resulting from inaccuracies or omissions. The specifications contained in this document are subject to change without notice.

SafeNet, SafeNet Authentication Manager and SafeNet Authentication Client are either registered with the U.S. Patent and Trademark Office or are trademarks of SafeNet, Inc., and its subsidiaries and affiliates, in the United States and other countries. All other trademarks referenced in this Manual are trademarks of their respective owners.

SafeNet Hardware and/or Software products described in this document may be protected by one or more U.S. Patents, foreign patents, or pending patent applications.

Please contact SafeNet Support for details of FCC Compliance, CE Compliance, and UL Notification.

Date of Publication: May 2011
Last update: February 2012
Contacting SafeNet

We work closely with our reseller partners to offer the best worldwide technical support services. Your reseller is the first line of support when you have questions about products and services. However, if you require additional assistance you can contact the SafeNet technical support team help-desk which is available 24 hours a day, seven days a week:

<table>
<thead>
<tr>
<th>Country/Region</th>
<th>Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>+1-800-545-6608</td>
</tr>
<tr>
<td>International</td>
<td>+1-410-931-7520</td>
</tr>
</tbody>
</table>

For further assistance submit additional questions to the SafeNet technical support team at the following web page:

http://c3.safenet-inc.com/secure.asp

For assistance via email to SafeNet technical support send the request to the following address:

support@safenet-inc.com
Introduction

SafeNet Authentication Manager (SAM) enables management of the complete user authentication life cycle. SafeNet Authentication Manager links tokens with users, organizational rules, and security applications to allow streamlined handling of users needs throughout the various stages of their authentication lifecycle.

VeriSign Managed PKI provides all of the essential security services needed for establishing trust in online electronic transactions.

The SAM 8.0 SP1 Hotfix 110.30 enables the use of certificates supplied by the VeriSign Certification Authority (CA).

The VeriSign has a Managed PKI Control Center site that sets the enrolled certificate policy.

In this section:

• Overview of VeriSign Managed PKI Control Center
Overview

VeriSign Managed PKI Service is a PKI certificate management and authentication service that runs on VeriSign's globally managed, and highly reliable infrastructure. Quick to deploy and easily integrated into the existing network infrastructure, VeriSign Managed PKI Service is optimized for heterogeneous operating system environments, homogeneous Windows and Active Directory environments, and non-PC based devices including ATMs, printers, telecommunications, and networking equipment.

This document describes how to configure VeriSign managed PKI policy to work with SAM.
Configure VeriSign Managed PKI Policy

This section describes how to configure the VeriSign Managed PKI policy. Some of the configurations are relevant only for the VeriSign site and are not used by SAM. However, these configurations have to meet your internal needs.

To configure the VeriSign Managed PKI policy:

1. Login to your VeriSign Manage PKI policy site using the certificate provided to you by VeriSign. The Managed PKI Control Center site opens.

2. From the top menu, click the Configuration link. The Configuration page opens with configuration options on the left.

3. Click the Policy link on the left. Step 1 opens (Enter the Email Address for Certificate Questions).
4. In the Email address for subscriber support field, enter the support email address.

5. Click **Continue**. Step 2 opens (Specify the Cryptographic Service Provider Name and Key Size).

6. Select **Use a Microsoft CSP module**. Choose any CSP from the drop-down list.
   - **Specify a Key Size** – Choose the key size to be enrolled, this must fit the token’s compatability.
   - **Key Exportable** – Choose whether you want the private key to be exportable (Required for key backup in SAM).

7. Click **Continue**. Step 3 opens (Specify the Security Feature for Subscriber’s Private Key).
8. As SAM is responsible for keeping the private keys; select *Rely on Windows logon security to protect the private key.*

9. Click **Continue.** Step 4 opens. *(Specify the Encoding for Certificate Content).*

10. If you are not using IPSec Certificates, select **UTF-8 Encoding** from the *Encoding* drop-down list. If you are using IPSec Certificates, select **No UTF-8 Encoding** from the drop-down list.

11. Click **Continue.** Step 5 opens. *(Specify the Authentication Method).*
12. As SAM enables users to authenticate and enroll the right certificate to the appropriate user, there is no need for the administrator to review the requests, therefore select the **Automated Administration** option.

13. Choose **Continue**. Step 6 opens. (Enter Local Hosting Base URL).

14. Enter a URL in the **Local Hosting Base URL** field (This is not relevant for SAM, so it does not matter which URL is entered).

   **Note:** This value cannot be empty.

15. Click **Continue**. Step 7 opens. (Customize the Subscriber Enrollment Page).
16. As this page is not relevant to SAM, we recommend that you select all the check boxes, and set all the options to **Optional** (this prevents failure when there is no data in the user repository).

17. Click **Continue. Step 8 opens. (Customize the Subscriber Certificates)**.

18. Check the data that you want displayed under **Subject** in the enrolled certificates **Details** tab.

19. Click **Continue. Step 9 opens. (Certificate Publishing Policy)**.
20. Select **Always Publish** to publish your certificates or the **Never Publish** option to avoid publishing the certificates. To allow SAM TPO configuration to set this option, select **Allow Subscriber to Decide**.

21. Click **Submit**. The system has saved your configuration settings window is displayed.