SafeNet Authentication Client
Integration Guide

Using SAC 8.3 with Entrust Authority™ 8.1
Document Information

| Product Version | Entrust Authority™ 8.1  
|                 | SAC 8.3               |
| Document        | Revision C            |
| Release Date    | February 2014         |

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
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 SafeNet Customer Support. SafeNet 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 SafeNet 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>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017</td>
</tr>
<tr>
<td></td>
<td>USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>United States 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 1-410-931-7520</td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td><a href="mailto:support@safenet-inc.com">support@safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Support and Downloads</strong></td>
<td><a href="http://www.safenet-inc.com/Support">www.safenet-inc.com/Support</a></td>
</tr>
<tr>
<td></td>
<td>Provides access to the SafeNet Knowledge Base and quick downloads for various products.</td>
</tr>
<tr>
<td><strong>Technical Support Customer Portal</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td></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 SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>
## Contents

- Description .............................................................................................................................................. 6
- Audience .................................................................................................................................................. 6
- Integration System Requirements ............................................................................................................. 6
  - Required Software ............................................................................................................................... 6
  - Supported Tokens ................................................................................................................................. 7
- Entrust Authority Security Manager Overview .......................................................................................... 7
- SafeNet Authentication Client Overview ................................................................................................... 7
- SafeNet Authentication Manager and Entrust Integration ......................................................................... 8
- Managing Logon Certificates for Tokens ................................................................................................. 9
  - Configuring the eToken CSP for Smart Card Logon Certificates ....................................................... 9
  - Activating Users for Smart Card Logon Certificates ......................................................................... 10
- Managing Two Key-Pair Certificates for Token Use ............................................................................... 12
  - Configuring the eToken CSP for Two Key-Pair Certificates ............................................................. 12
  - Activating Users for Two Key-Pair Certificates ............................................................................... 13
- Enrolling a Certificate to a Token ........................................................................................................... 14
- Recovering a Certificate .......................................................................................................................... 15
  - Administrator’s Role in Certificate Recovery .................................................................................. 15
  - User’s Role in Certificate Recovery .................................................................................................. 16
- Preparing for Profile Logon to Security Manager Administration .............................................................. 17
  - Configuring a Security Officer Profile ............................................................................................ 17
  - Logging On to Security Manager Administration with a Profile ..................................................... 18
Description

This guide describes how to enable SafeNet tokens with certificates generated by Entrust Authority Security Manager 8.1 for use with SafeNet Authentication Client 8.3 in a Windows environment.

Private keys are stored on the users' tokens, ensuring that the users' digital identities are not jeopardized, and that hostile entities cannot use a stolen digital identity to penetrate the corporate environment. Generating and keeping private keys on tokens ensures a high level of security. When a SafeNet token is connected to the client workstation, the certificate stored on the token is available for use with various supported authentication solutions.

To store smart card certificates on your organization's SafeNet tokens, use Entrust Security Manager to tailor the appropriate certificate definition policy.

Entrust Security Provider 9.2 supports full Public Key Infrastructure (PKI) authentication based on a private key. The private key can be generated and protected by a SafeNet token, reducing the vulnerability of the digital identity. A user needs only to present the certificate stored on the token to authenticate successfully or to perform any other secured operation.

An Entrust profile is similar to a digital certificate. It contains essential information about the user, such as the user name and keys, in encrypted form.

Audience

This document is intended for those responsible for data security and integrity in an organization that uses Entrust Authority Security Manager 8.1, Entrust Entelligence™ Security Provider 9.2 and SafeNet Authentication Client 8.3 interoperability.

Integration System Requirements

Required Software

- Entrust Authority Security Manager 8.1 modules:
  - Security Manager
  - Security Manager Administration
  - Security Manager database
- Microsoft Active Directory
- Windows 7/XP clients with Entrust Entelligence™ Security Provider 9.2 installed
- SafeNet Authentication Client (SAC) 8.3 installed on the following:
  - the computer which runs Security Manager Administrator
  - Windows 7/XP clients
**Supported Tokens**

SafeNet Authentication Client 8.3 supports the following tokens:

- SafeNet eToken 7300 (Standard 0x6002 and HID PID 0x3005)
- SafeNet eToken 5100/5105 (SafeNet eToken PRO)
- SafeNet eToken 5200/5205 (SafeNet eToken PRO Anywhere)
- SafeNet eToken 5200/5205 HID
- SafeNet eToken 4100 (SafeNet eToken PRO Smartcard)
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)
- SafeNet eToken 7100 (SafeNet eToken NG-Flash)
- SafeNet eToken 7200 (SafeNet eToken NG-Flash Anywhere)
- SafeNet eToken Virtual Family
- SafeNet iKey: 2032, 2032u, 2032i
- SafeNet Smartcard: SC330, SC330u, SC330i
- SafeNet Smartcard SC400
- SafeNet iKey 4000

**Entrust Authority Security Manager Overview**

**Entrust Authority Security Manager** is the Certification Authority (CA) in a public key infrastructure. Security Manager provides the capabilities of a traditional CA together with advanced features necessary to help facilitate administration.

The main functions of Security Manager are:

- Create certificates for all public keys.
- Create encryption key pairs for users.
- Manage a secure database of information that allows the recovery of users’ encryption key pairs (for example, if a user forgets the password).
- Enforce the security policies defined by the organization.

**SafeNet Authentication Client Overview**

**SafeNet Authentication Client** (SAC) is Public Key Infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities.

SafeNet Authentication Client enables the implementation of strong two-factor authentication using standard certificates as well as encryption and digital signing of data.

SAC incorporates features that were supported by previous releases of eToken PKI Client and SafeNet Borderless Security (BSec). It provides a unified middleware client for a variety of SafeNet smartcards and devices, SafeNet iKey tokens, and SafeNet eToken authenticators.
SAC’s generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications offering secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely from within hardware or software tokens.

The certificate type can be set as Key Storage Provider (KSP) or Cryptographic Service Provider (CSP).

SafeNet provides a mechanism that allows administrators to prevent the use of legacy or obsolete algorithms by third-party applications. When this mechanism is enabled, SAC considers the following cryptographic algorithms as obsolete:

MD5, RC2, RSA<1024, DES, GenericSecret<80, RC4<80, ECC<160, ECB, RSA-RAW.

SafeNet Authentication Client includes support for the following:

- Standard PKCS#11 implementation API for eToken and iKey tokens
- Standard CAPI implementation for eToken and iKey tokens
- Smart Card KSP provider
- Legacy iKey CAPI applications
- Legacy iKey PKCS#11 applications

SafeNet Authentication Client and Entrust Integration

SafeNet Authentication Manager (SAM) provides your organization with a comprehensive platform to manage all of your authentication requirements, across the enterprise and the cloud, in a single, integrated system.

SAM enables management of the complete user authentication lifecycle. SAM links tokens with users, organizational rules, and security applications to allow streamlined handling of your organization's authentication infrastructure with a flexible, extensible, and scalable management platform.

SafeNet Authentication Manager 8.2 supports the following user stores:

- Microsoft Active Directory (Windows Server 2003 or Windows Server 2008)
- AD LDS and ADAM (in an integrated configuration solution using a Standalone user store)
- Remote Active Directory
- Microsoft SQL Server 2005 / 2008
- OpenLDAP
- Novell eDirectory

For more information, refer to the SafeNet Authentication Manager 8.2 Administrator Guide.

Integrating SAM infrastructure with Entrust Authority Security Manager’s PKI functionality enables the seamless integration of Entrust-based certificate and key lifecycle management in the SAM token management and enrollment websites.

The SAM Connector for Entrust offers the following benefits:

- Provides seamless integration between SafeNet Authentication Manager and the Entrust CA. Through the SAM infrastructure, token users enroll certificates issued by Entrust, and generate private keys on tokens.
- Enables Entrust customers to manage PKI lifecycle operations, including key enrollment, key revocation, key recovery, and re-enrollment, through the SAM Management Center and the SAM Self Service Center.
- Allows automated certificate renewal, as well as the change and addition of key pairs, through the SAM Remote Service Center, the SAM Management Center, and the SAM Self Service Center.
• Supports the SAM “employee on the road” solution, which provides users with continued access to computers and networks after losing or damaging their token.

• Enables the configuration of TPO settings to control the automated enrollment of certificates to tokens based on specific groups of users.

• Allows automated user provisioning into the Entrust CA.

• Requires only that the SafeNet Authentication Manager client be installed, and not the Entrust client, to enroll Entrust certificates to a token.

• Enables the auditing of Entrust-related PKI operations performed using the SAM Connector for Entrust.

Managing Logon Certificates for Tokens

In your organization, users may be required to connect their tokens while logging on, so that their logon certificates can be read and authenticated.

Use Entrust Authority to prepare smart card logon certificates for enrollment on users’ tokens.

Enabling smart card logon entails:
A. Configuring the eToken CSP for Smart Card Logon Certificates
B. Activating Users for Smart Card Logon Certificates
C. Enrolling a Certificate to a Token

Configuring the eToken CSP for Smart Card Logon Certificates

To configure the eToken CSP for smart card logon certificates:


2. In the Policy mapping tab’s Certificate definition Policy field, select Dual Usage No Key Backup Policy.
3. Click **Apply**, and then confirm and authorize the changes.


5. In the **Policy Attributes** section, scroll down until the field **CSP to manage keys** appears, and enter **eToken Base Cryptographic Provider**.

   **NOTE:** If your organization runs SAC in BSec-Compatible mode, enter **safenet rsa csp** instead of **eToken Base Cryptographic Provider**.

6. Click **Apply**, and then confirm and authorize the changes.

**Activating Users for Smart Card Logon Certificates**

**To activate users in the Entrust environment:**

1. In the **Security Manager Administration** console tree, right-click **Users**, and select **Find > By Directory Attributes**.

   The **Find Users by Directory Attributes** window opens.

2. Select **User**, and click **Find**.

   The list of users opens in the **Security Manager Administration** console’s right pane.
3. In the list of users, right-click the *Distinguished Name* of the user to enroll for SafeNet token authentication, and select **Properties**.

The *User Properties* window opens.

4. In the *Certificate Info* tab, select the *Certificate Type* **Smart Card Logon for MS Security Framework Users**.

![User Properties Window](image)

5. Click **OK**, and then confirm and authorize the changes.

When a certificate is generated for a new user, **Reference number** and **Authorization code** details for this user are generated and displayed.

![Operation Completed Successfully](image)

6. Record the details. They will be needed in step 3 of *Enrolling a Certificate to a Token*.

7. To view the **Reference number** and **Authorization code** details needed in step 3 of *Enrolling a Certificate to a Token*, perform steps 1 to 3, and select the **Activation Codes** tab.

The **Reference number** and **Authorization code** details that were generated for this user are displayed.

![User Properties with Activation Codes](image)

To enroll the smart card logon certificate on the user’s token, see *Enrolling a Certificate to a Token*. 
Managing Two Key-Pair Certificates for Token Use

In your organization, users may be required to connect their tokens for encryption, verification, signing, and other authentication tasks, so that their Two Key-Pair certificates can be read and authenticated.

Use Entrust Authority to prepare Two Key-Pair certificates for enrollment on users’ tokens.

Enabling Two Key-Pair certificates entails:
A. Configuring the eToken CSP for Two Key-Pair Certificates
B. Activating Users for Two Key-Pair Certificates
C. Enrolling a Certificate to a Token

Configuring the eToken CSP for Two Key-Pair Certificates

To configure a Two-Key-Pair user on eToken CSP:

1. In the Security Manager Administration console tree, and navigate to User Policies > Encryption Policy, and select the General Information tab.
2. In the Type area, select Cert. Defn. Settings.
3. In the Policy Attributes section, scroll down until the field CSP to manage keys appears, and enter eToken Base Cryptographic Provider.
4. Click Apply, and then confirm and authorize the changes.
5. In the Security Manager Administration console tree, navigate to User Policies > Verification Policy, and select the General Information tab.
6. In the Type area, select Cert. Defn. Settings.
7. In the Policy Attributes section, scroll down until the field CSP to manage keys appears, and enter eToken Base Cryptographic Provider.

NOTE: If your organization runs SAC in BSec-Compatible mode, enter safenet rsa csp instead of eToken Base Cryptographic Provider.
8. Click **Apply**, and then confirm and authorize the changes.

## Activating Users for Two Key-Pair Certificates

**To activate the user in the Entrust Environment:**

1. In the *Security Manager Administration* console tree, right-click **Users**, and select **Find > By Directory Attributes**.
   
   The *Find Users by Directory Attributes* window opens.

   ![Find Users by Directory Attributes](image)

2. Select **User**, and click **Find**.
   
   The list of users opens in the *Security Manager Administration* console’s right pane.

3. In the list of users, right-click the **Distinguished Name** of the user to enroll for SafeNet token authentication, and select **Properties**.

   The *User Properties* window opens.

4. In the *Certificate Info* tab, select the **Certificate Type 2-Key-Pair User**.

   ![User Properties](image)

5. Click **OK**, and then confirm and authorize the changes.

   When a certificate is generated for a new user, **Reference number** and **Authorization code** details for this user are generated and displayed.
6. Record the details. They will be needed in step 3 of Enrolling a Certificate to a Token.

7. To view the Reference number and Authorization code details needed in step 3 of Enrolling a Certificate to a Token, perform steps 1 to 3, and select the Activation Codes tab.

The Reference number and Authorization code details that were generated for this user are displayed.

To enroll the certificate on the user’s token, see Enrolling a Certificate to a Token.

**Enrolling a Certificate to a Token**

The following components must be installed on every enrollment station:

- SafeNet Authentication Client 8.3
- Entrust Entelligence™ Security Provider 9.2

To enroll a certificate to a token:

1. Connect the SafeNet token to the enrollment workstation running SafeNet Authentication Client 8.3. Depending on the token model, this may entail inserting the USB token into a USB port.

2. Go to Start > All Programs > Entrust Entelligence > Enroll for Entrust Digital ID.

The Enroll for Entrust Digital ID Wizard opens.
3. Enter the Reference number and Authorization code that was generated by the Security Manager Administration.

4. Click Next to begin the enrollment procedure.
   You are prompted to enter the token’s Token Password.

5. Enter the Token Password, and click OK.
   The enrollment process continues until the wizard completes.

   The certificate is stored on the token.

---

## Recovering a Certificate

When a Digital ID Certificate must be recovered, the administrator begins the certificate recovery process by generating replacement Reference number and Authorization code details using the Security Manager Administration console.

Then the user uses the generated details to complete the certificate recovery process.

---

### Administrator’s Role in Certificate Recovery

To perform the administrator’s role that begins certificate recovery:

1. To generate activation codes for recovery, open the Security Manager Administration console tree, right-click Users, and select Find > By Directory Attributes.
   The Find Users by Directory Attributes window opens.

2. Select User, and click Find.
   The list of users opens in the Security Manager Administration console’s right pane.

3. In the list of users, right-click the Distinguished Name of the user to be recovered, and select Begin Key Recovery.

4. Authorize the changes.
   The Reference number and Authorization code details for this user are displayed.
5. Record the details. They will be needed in step 3 of User’s Role in Certificate Recovery.

**User’s Role in Certificate Recovery**

To perform the user’s role that completes certificate recovery:

1. Ensure that the user’s token is connected to the client workstation running SafeNet Authentication Client 8.2, and log on as the user to whom the token is enrolled.

2. Go to **Start > All Programs > Entrust Entelligence > Recover Entrust Digital ID**.

The **Recover Entrust Digital ID Wizard** opens.

3. Enter the **Reference number** and **Authorization code** generated when the administrator began certificate recovery. See step 5 of Administrator’s Role in Certificate Recovery.

4. Click **Next** to begin the enrollment procedure.
   
   You are prompted to enter the token's Token Password.

5. Enter the Token Password, and click **OK**.
   
   The enrollment process continues until the wizard completes.
   
   A replacement certificate is stored on the token.
Preparing for Profile Logon to Security Manager Administration

In your organization, Security Manager Administration managers having the Security Officer role may be required to connect their tokens while logging on to Security Manager Administration so that their profiles can be read and authenticated.

The following rules apply when a token is used for logging on to Security Manager Administration:

- SafeNet Authentication Client 8.3 must be installed on the computer which runs Security Manager Administrator.
- When using a token to log on to Security Manager Administration, the token must remain connected (for example, in the reader) for Security Manager Administration to continue running.
- No more than two tokens can be connected at a time to the Security Manager Administration computer.
- Security Manager Administration supports only one vendor library at a time.

Configuring a Security Officer Profile

To create a Security Officer profile on a token for Security Manager Administration management:

1. On the Security Manager Administration computer running SafeNet Authentication Client 8.2, go to C:\Program Files (x86)\Entrust\Security Manager Administration, and open file entrust.ini for editing.
2. Under the [Entrust Settings] section, add or configure the following to the CryptokiV2LibraryNT setting so that it points to the path of the hardware device driver:
   
   ```
   Version=8.1
   CryptokiV2LibraryNT=etpkcs11.dll
   CryptokiV2Library95=etpkcs11.dll
   ```
3. Restart the Security Manager.
4. Log on to Security Manager Administration.
5. Ensure that the token to contain the Security Officer profile is connected.
6. In the Security Manager Administration console tree, right-click Users, and select Find > By Directory Attributes.
   
   The Find Users by Directory Attributes window opens.
7. Select User, and click Find.
   
   The list of users opens in the Security Manager Administration console’s right pane.
8. In the list of users, right-click the Distinguished Name of a user who is assigned the Security Officer role, and select Create Profile.
   
   The Select profile storage location window opens.
9. Click Yes to store the profile on the connected token.
The Create Profile window opens.

10. In the Name field, enter a friendly name for the profile. The name can be up to 75 characters long.

11. In the PIN field, enter the Token Password, and click OK.

12. If the token already contains a profile, a message is displayed asking if you want to overwrite the existing profile.

   Click No to cancel the profile creation, or click Yes to overwrite the existing profile.

   The profile and its Entrust support files are written to the token.

Logging On to Security Manager Administration with a Profile

To use a profile to log on to Security Manager Administration:

1. Connect the token containing the Security Officer profile.

2. Go to Start > All Programs > Entrust > Security Manager Administration, or use desktop shortcut icon.

   The Entrust Authority (TM) Security Manager Administration Log In window opens.

3. Enter the eToken Password, and click OK.