SafeNet Authentication Client

Compatibility Guide

Using SAC CBA for OpenTrust

gemalto
security to be free

Release Date: September 2017

Document Number: 007-013815-001

Contents

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC)** - SAC 10.4 standard mode with IDGo800 PKCS11
- **SafeNet Authentication Client (SAC) IDGo800 Compatible mode** - with eToken drivers installed side-by-side.

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Client (SAC)** - with IDGo800 PKCS11 - See Figure 1
- **SafeNet Authentication Client (SAC) IDGo800 Compatible mode** - with eToken drivers installed side-by-side. See Figure 2
- **OpenTrust CMS client 4.9.2**
- **OpenTrust server 4.10**

Tested Tokens

SAC supports a number of tokens that can be used as a second authentication factor for users who authenticate to OpenTrust Client.

Below is the list of devices tested with OpenTrust Client:

Certificate-based USB tokens

- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 GA
- SafeNet eToken 5110 CC

Smart Cards

- IDprime MD 840 Rev B
- IDprime MD 830 Rev B
- IDprime MD 830
- IDprime MD 840

USB Smart Card Reader

- Gemalto CT 40

SAC Installation

The SAC 10.4 installation package must be generated using the SAC customization tool.

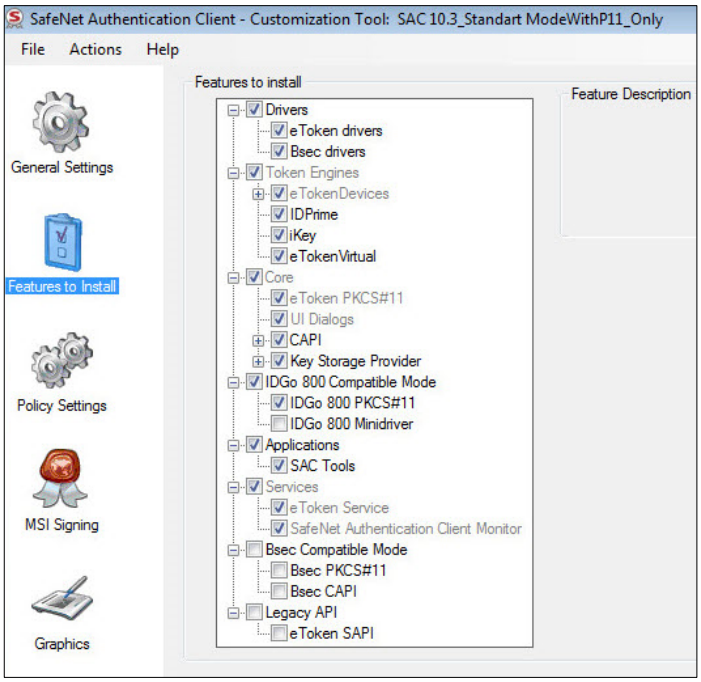

Figure 1: SafeNet Authentication Client (SAC) with IDGo800 PKCS11 10.4

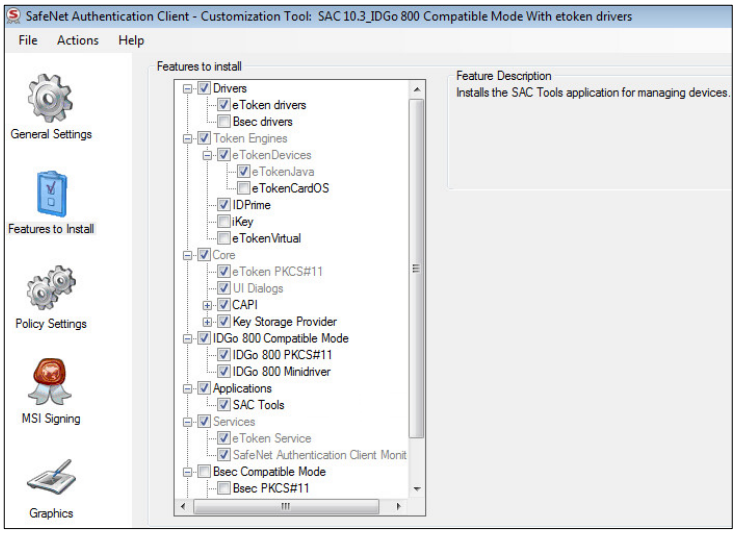

Figure 2: SafeNet Authentication Client (SAC) IDGo800 Compatible mode with eToken driver side-by-side package

NOTE: When selecting the IDGo 800 Minidriver option, several options are automatically cleared. Ensure that eTokenJava is selected.

Configuring SAC

In order to work on the same OpenTrust client machine with both IDPrime MD cards and eToken devices, the registry keys below are used to assist OpenTrust client distinguish between our products and their specific behavior.

After installing SAC, add the ApiMode registry to the SAC Registry.

Perform the following on Windows 32 –bit system:

1. Create the **General** Key under:
   HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC
2. Create the **otscm-client.exe** key under:
   HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\General
3. Create the entry **ApiMode** of type **REG_DWORD**, with the value **6** under:
   HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\General\otscm-client.exe

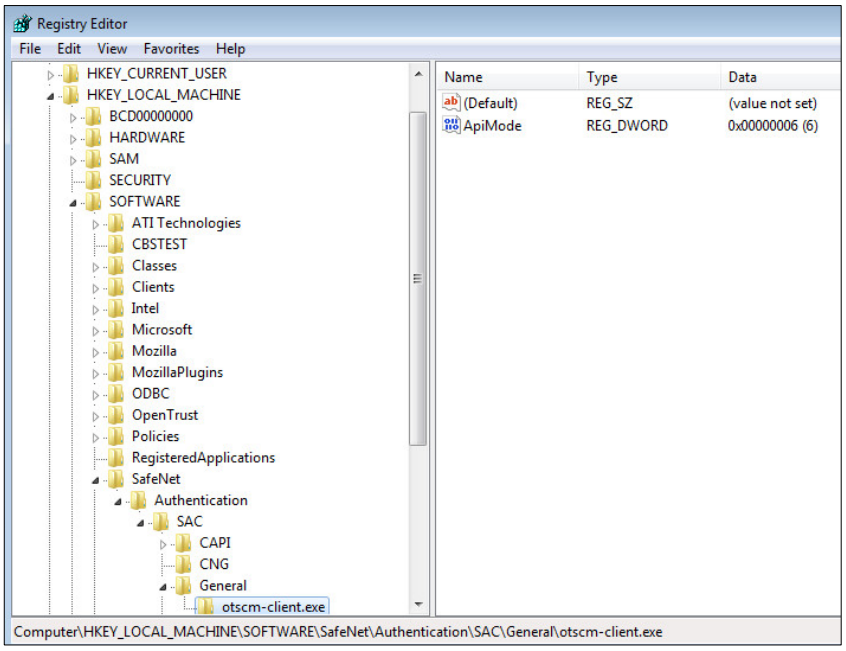

Figure 3: ApiMode registry added on a Windows 32 –bit system

Perform the following on Windows 64 –bit system (Sets both registries x32 and x64):

1. Create the **General** key under:
   HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC
2. Create the **otscm-client.exe** key under:
   HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\General
3. Create the entry **ApiMode** of type **REG_DWORD**, with the value **6** under:
   HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\General\otscm-client.exe

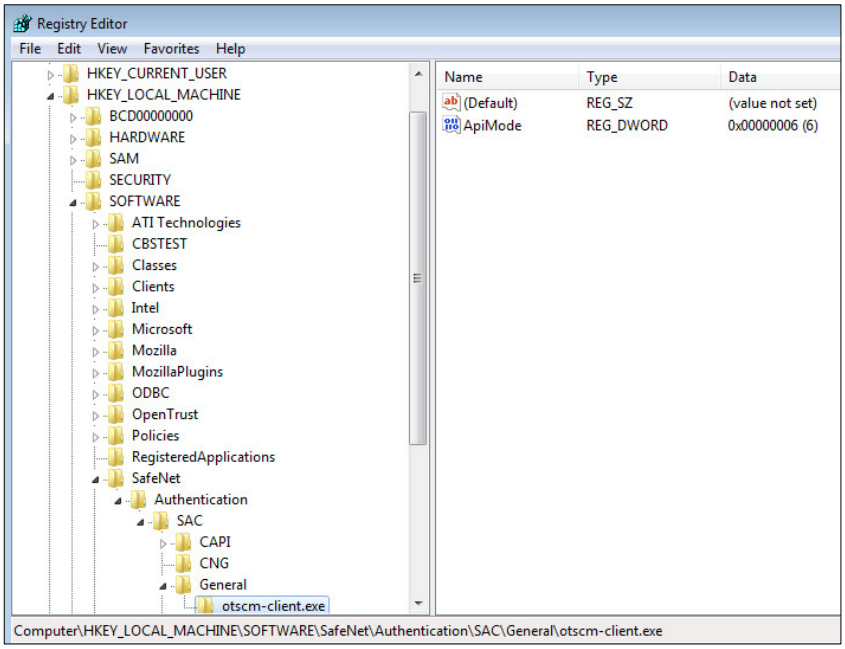

Figure 4: ApiMode registry added on a Windows 64 –bit system

Perform the following on Wow64 –bit system:

1. Create the **General** key under:
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SafeNet\Authentication\SAC
2. Create the **otscm-client.exe** key under:
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SafeNet\Authentication\SAC\General
3. Create the entry **ApiMode** of type **REG_DWORD**, with the value **6** under:
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SafeNet\Authentication\SAC\General\otscm-client.exe

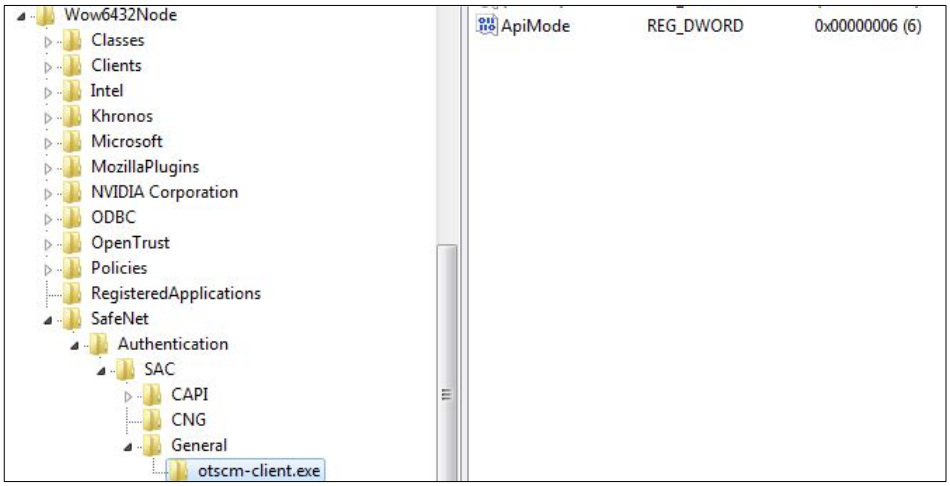

Figure 5: ApiMode registry added on a Wow 64 –bit system

Validated Use Cases with SAC

The following use cases were validated:

- Self-enrollment with card initialization
- Self-unlock
- User PIN change
- SSL authentication to Web https://cms-demo.idnomic.net/
- Authoritative offline unlock:
  - SAC Tools generates the **Challenge Code**.
  - Copy and paste the **Challenge Code** on the server side and get the **Response Code**.
  - Paste the **Response Code** into **Unlock Token** window in SAC Tools to unlock the token (Not Supported with IDPrime MD 840 /SafeNet eToken 5110 CC)

Badge office enrollment was tested with 2 devices connected:

1. Operator - smart card (IDPrime MD 840) always connected.
2. Target User – can use either a smart card or token.
3. Badge office enrollment full test (tested with smart cards only).
4. Badge Unlock option.

Results

The following devices passed the above tests using SAC on win7x64 / x32:

- IDprime MD 840
- IDprime MD 840 B
- IDprime MD 830 B
- IDprime MD 830
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 GA
- SafeNet eToken 5110 CC

NOTE: When Minidriver support is not available, the following OpenTrust CMS functionalities are disabled:

- Card-initiated challenge/response admin authentication in OpenTrust CMS Client
- Card-related operations in the OpenTrust CMS Self-Care Web Portal

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.

Contact Method	Contact Information
Customer Support Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.
Technical Support contact email	technical.support@gemalto.com