SafeNet Authentication Client

Integration Guide

Using SafeNet Authentication Client CBA for Avencis SSOX

gemalto
security to be free

Document Number: 007-000153-001, Rev. A

Release Date: July 2018

Contents

Third-Party Software Acknowledgement 4
Description 4
Applicability 5
Environment 5
Audience 5
CBA Flow using SafeNet Authentication Client 6
Prerequisites 6
Supported Tokens and Smart Cards in SafeNet Authentication Client 7
Configuring Avencis SSOX 8
    SSOX Client Installation 8
    Configuring Certificate Template 10
    PKI Configuration on SSOX Server 11
    Configure Default Token Template 17
    Client Configuration: Configure the PKCS#11 path 21
Running the Solution 22
    Enroll a certificate on Token 22
    Authenticating to a Web Application 27
Support Contacts 28
    Customer Support Portal 28
    Telephone Support 28

Third-Party Software Acknowledgement

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

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

Remote access poses both a security and a compliance challenge to IT organizations. The ability to positively identify users (often remote users) requesting access to resources is a critical consideration in achieving a secure remote access solution. Deploying remote access solution without strong authentication is like putting your sensitive data in a vault (the datacenter), and leaving the key (user password) under the door mat.

A robust user authentication solution is required to screen access and provide proof-positive assurance that only authorized users are allowed access.

PKI is and effective strong authentication solution to the functional, security, and compliance requirements.

SafeNet Authentication Client (SAC) is a 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. Gemalto's certificate-based tokens and smart cards provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SafeNet Authentication Client (SAC). The SAC 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 with the hardware or software tokens.

Avencis SSOX, a solution offered under the France Cybersecurity brand, is a robust integrated access and monitoring solution (SSO) which guarantees the security of connections while also improving user experience.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Avencis SSOX using Gemalto's tokens and smart cards.

It is assumed that the Avencis SSOX environment is already configured and working with static passwords prior to implementing Gemalto multi-factor authentication.

Avencis SSOX can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with Gemalto products.

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC) Typical installation mode** - SafeNet Authentication Client is public key infrastructure (PKI) middleware that manages Gemalto's tokens and smart cards.
- **SafeNet Authentication Client (SAC) IDGo800 Compatible mode** - IDGo800 Minidriver based package, uses Microsoft Smart Card Base Cryptographic Provider to manage Gemalto IDPrime MD smart cards.

  For more details about different SAC installation modes, please refer to the customization section in the *SafeNet Authentication Client Administrator Guide*.
- **Avencis SSOX**

Environment

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

- **SafeNet Authentication Client (SAC)**— Version 10.5
- **Avencis SSOX**— Version 10.0.0.2

Audience

This document is targeted to system administrators who are familiar with Avencis SSOX, and are interested in adding multi-factor authentication capabilities using SafeNet tokens.

CBA Flow using SafeNet Authentication Client

The following diagram illustrates the flow of certificate-based authentication:

1. A user attempts to connect to the Avencis SSOX server using the Avencis SSOX client application. The user inserts the SafeNet token containing her certificate, and, when prompted, enters the token password.
2. After successful authentication, the user is allowed access to internal resources.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based authentication for Avencis SSOX using Gemalto tokens and smart cards:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. Any CA can be used. In this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, Token Policy Object (TPO) must be configured with MS CA Connector. For further details, refer to the section "Connector for Microsoft CA" in the *SafeNet Authentication Manager Administrator's Guide*.
- Users must have a Gemalto token or smart card enrolled with an appropriate certificate.
- SafeNet Authentication Client (Version 10.5) must be installed on all client machines.

Supported Tokens and Smart Cards in SafeNet Authentication Client

SafeNet Authentication Client (Version 10.5) supports the following tokens and smart cards:

Certificate-based USB tokens

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

Smart Cards

- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 840
- Gemalto IDCore 30 B

For a full list of supported devices, refer to *SafeNet Authentication Client Customer Release Notes*.

Configuring Avencis SSOX

> **NOTE:** In this document it is assumed that Avencis SSOX is installed and configured to work with LDAP authentication.

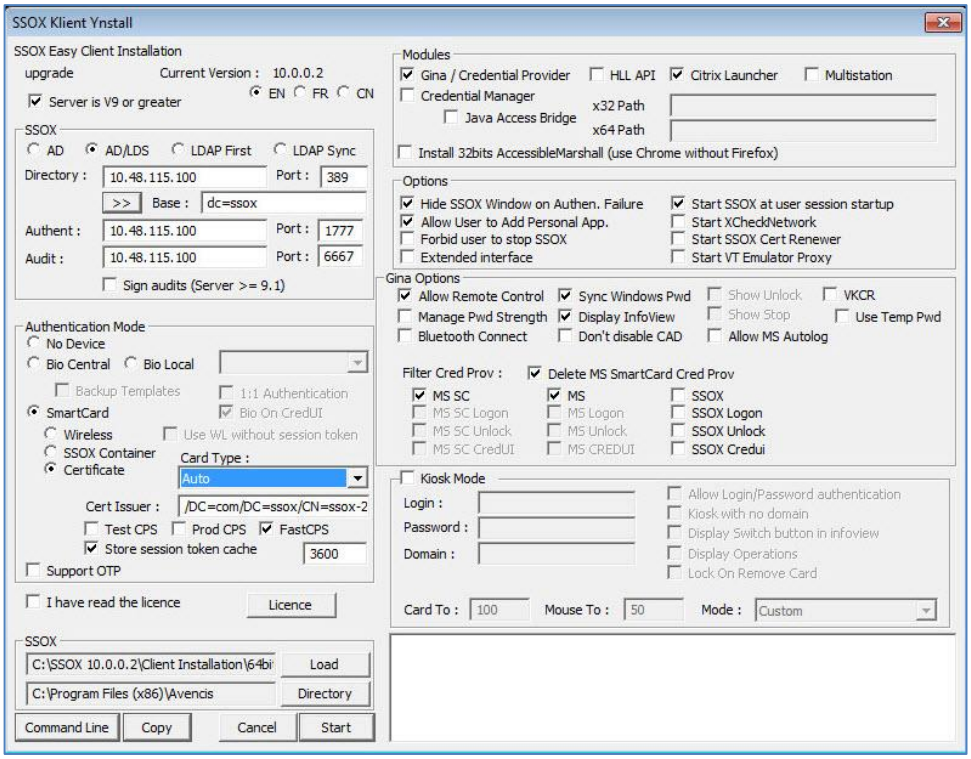
In the following section we will describe how to configure Avencis SSOX to work with SafeNet Authentication Client.

SSOX Client Installation

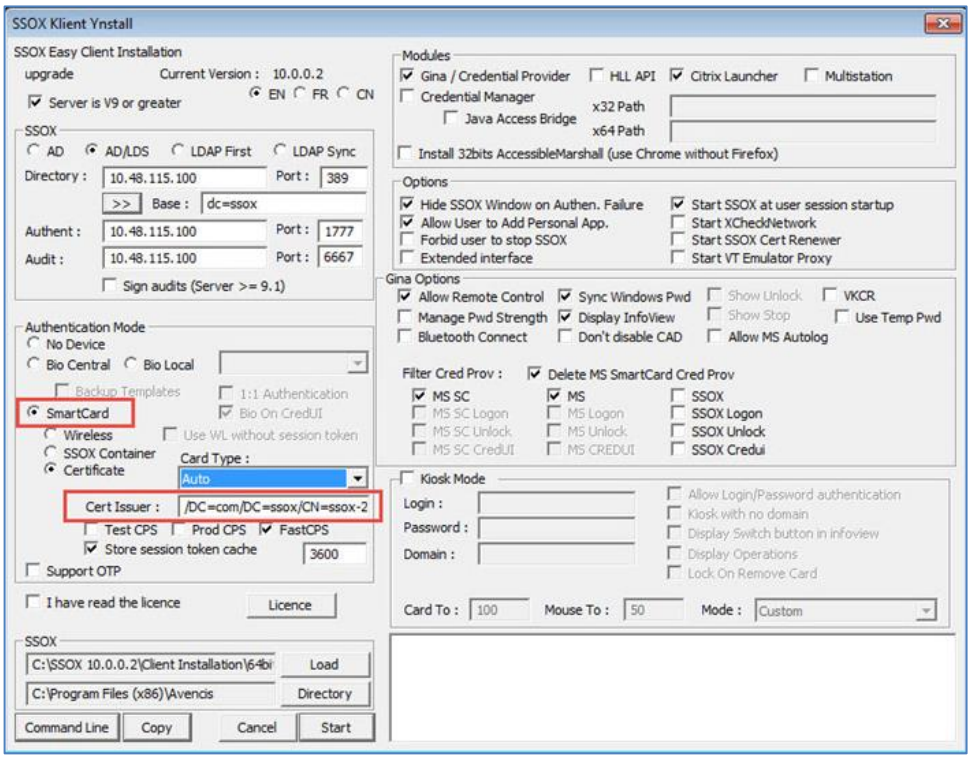
In this section we describe how to install SSOX client and configure it to support CBA using Gemalto smart cards and tokens.

1. Ensure that SAC is installed on the client.
2. Go to the SSOX installation folder and execute the file **sky.exe** with administrator rights (**Run as administrator**).

   The **SSOX Client Install** window opens.



3. Under **Authentication Mode** select **SmartCard** and then select **Certificate**.
4. Under **Certificate,** enter the appropriate **Cert Issuer.**

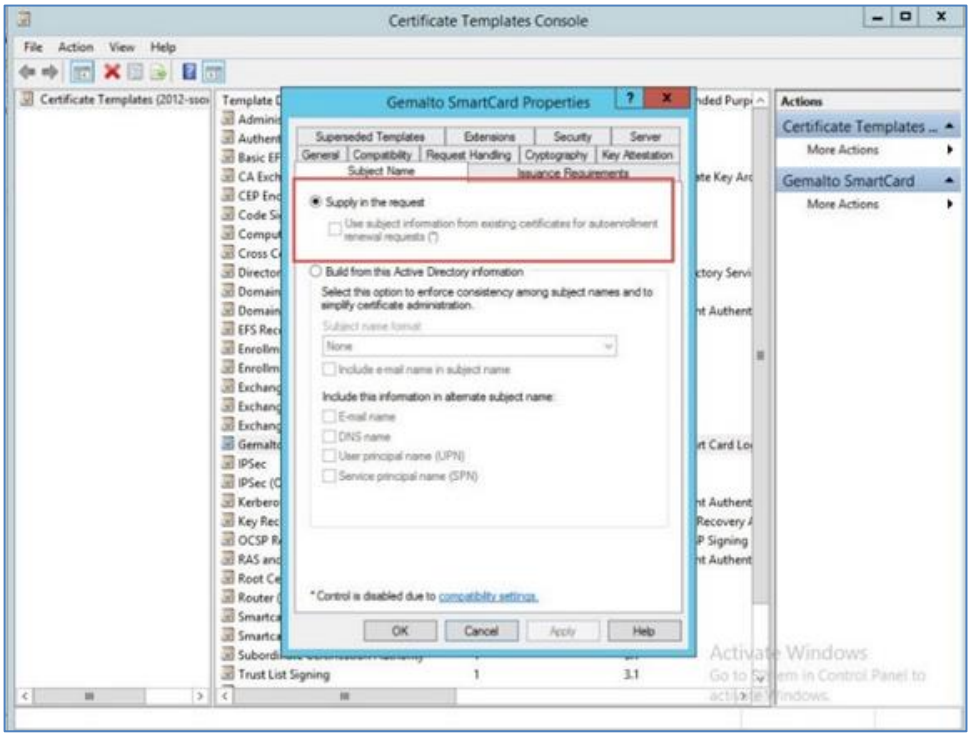


5. Click **Start** to install the SSOX client.

Configuring Certificate Template

For this integration, we use a Microsoft self-signed CA.

- When configuring the certificate template, in the **Gemalto SmartCard Properties** window, in the **Subject Name** tab, ensure that **Supply in the request** is selected.



PKI Configuration on SSOX Server

In this section, we will configure the SSOX server to work with PKI.

Prerequisites:

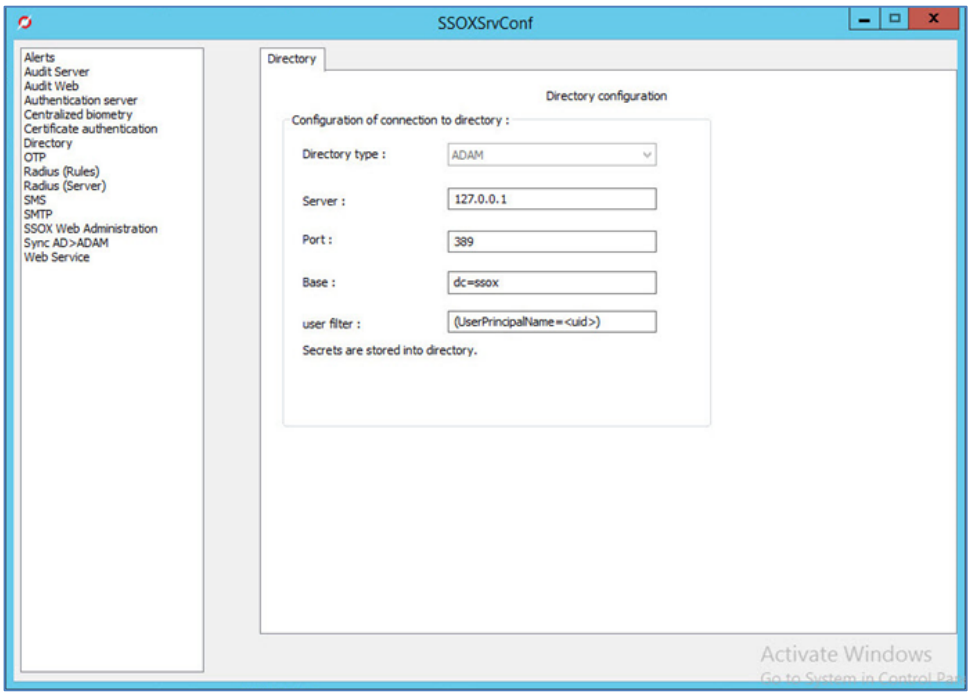
Create the following folders:

- **C:\Program Files (x86)\Avencis\SSOX Proxy\PKI\CA**
- **C:\Program Files (x86)\Avencis\SSOX Proxy\PKI\CRL**

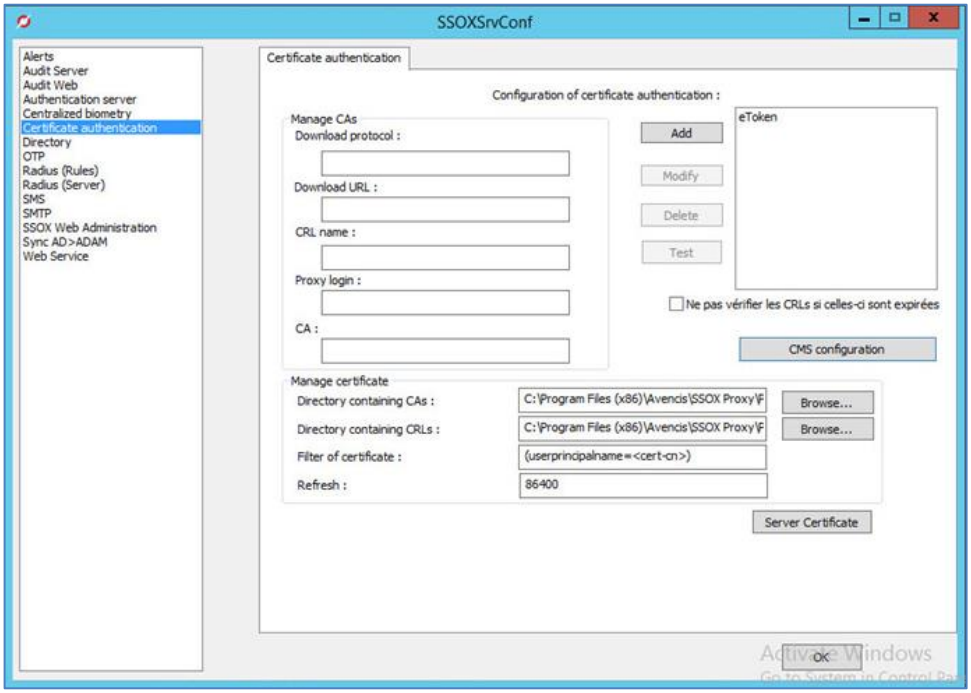
On the SSOX server:

1. In **C:\Program Files (x86)\Avencis\SSOX Administration,** execute the **SSOXSrvConf.exe** file.

   The SSOX Server configuration tool opens.

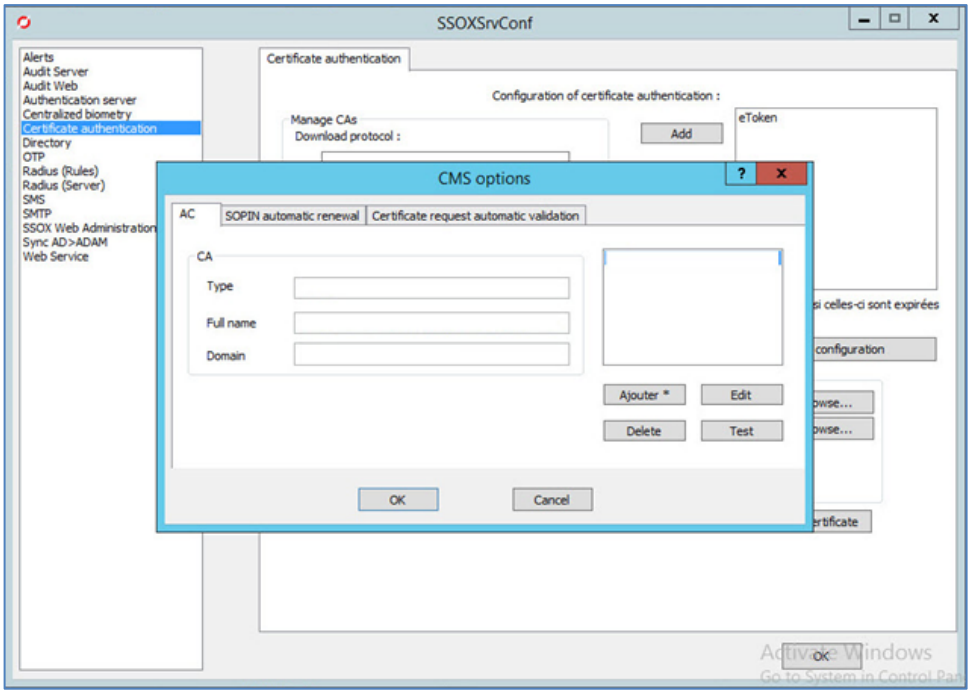


2. On the left pane select **Certificate authentication**



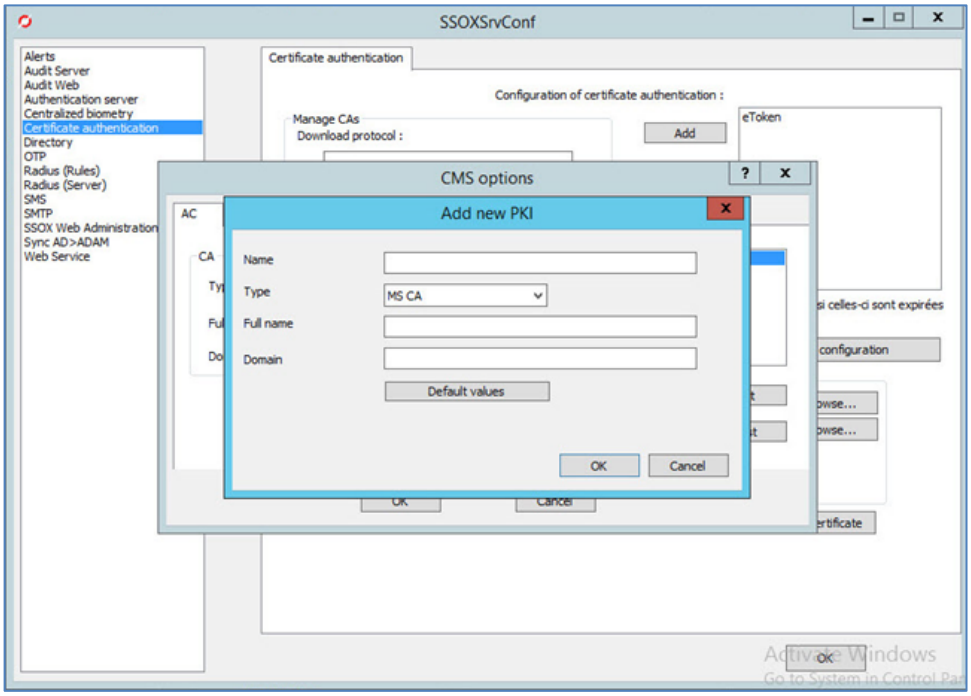
3. To add a new CMS record, click **CMS configuration**.

   The **CMS options** window opens.



4. Click **Add**.

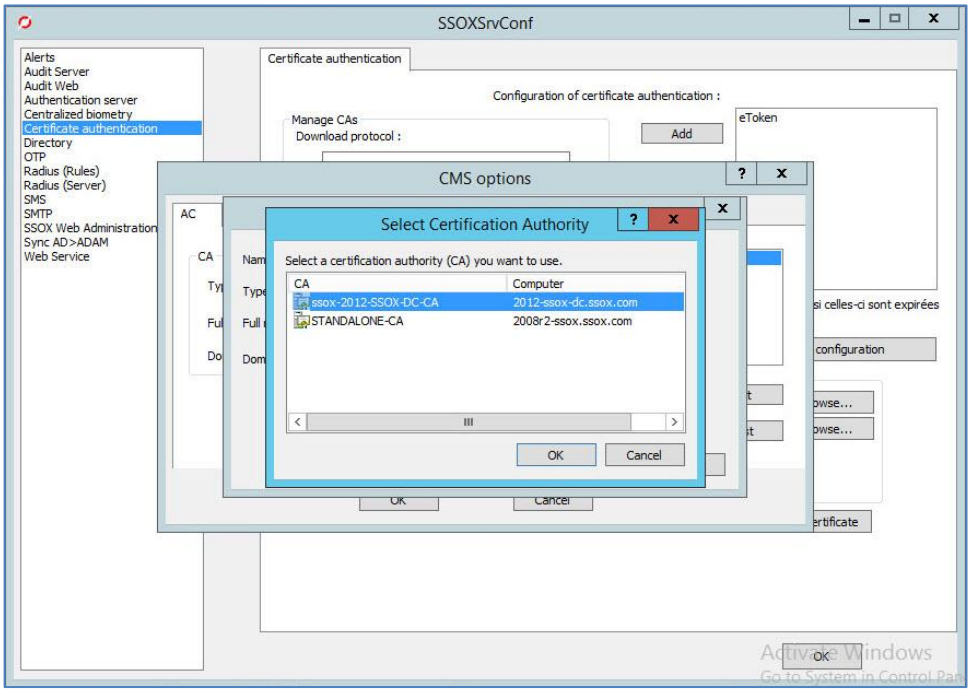
   The **Add new PKI** window opens.



   Now we will configure the CA.

5. Click **Default values**.

   The **Select Certification Authority** window opens.

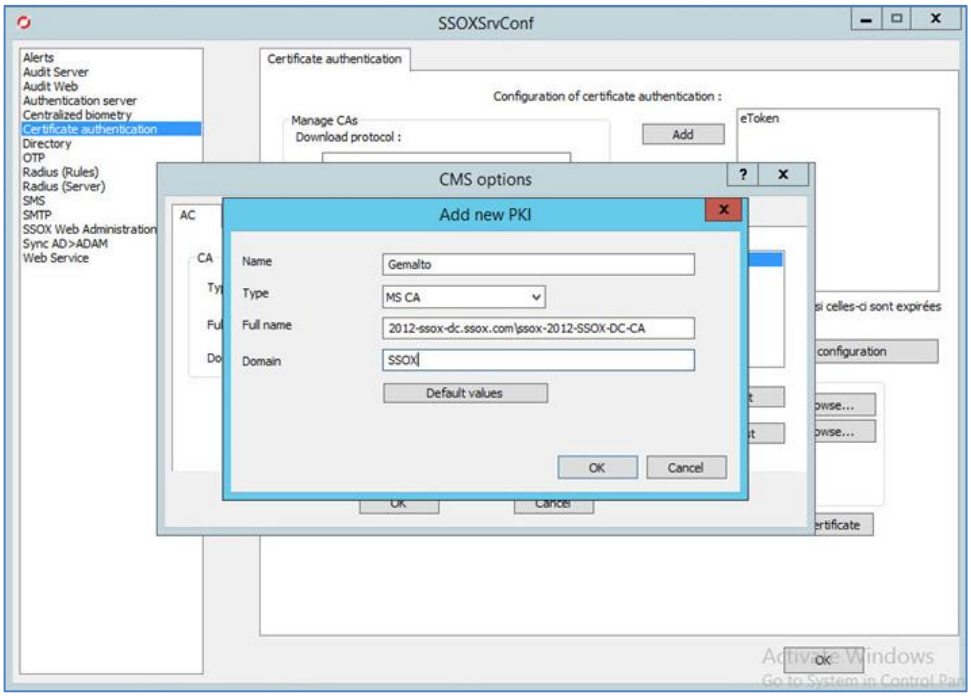


6. Select the Root CA certificate and click **OK**.

   The **Add new PKI** window opens

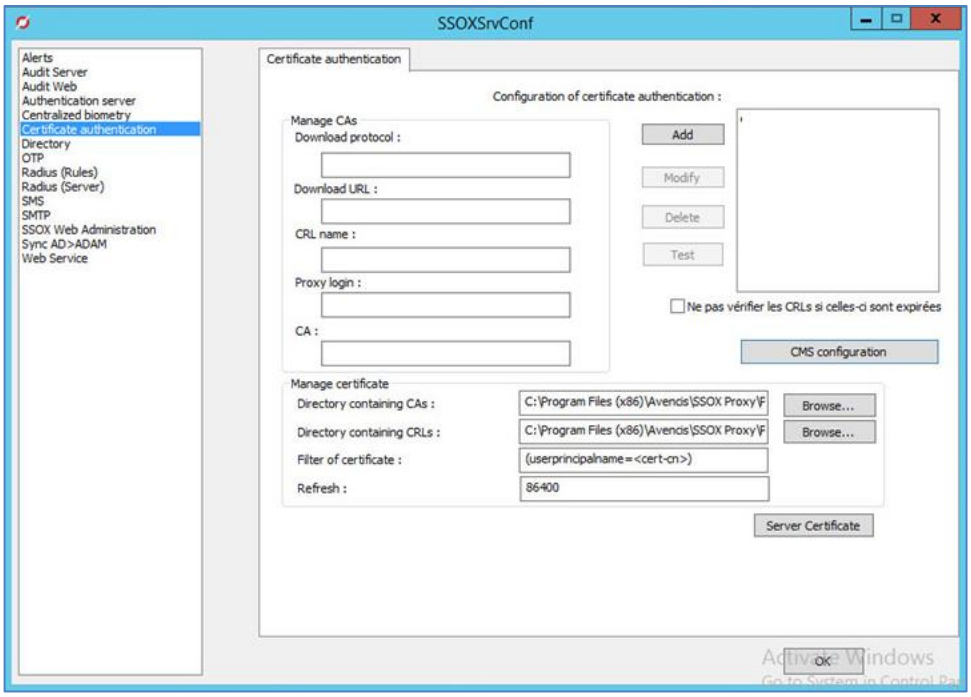
7. In the **Name** field, enter a name for the PKI rule and click **OK**.

8. After returning to the **CMS options** window, click **OK**.



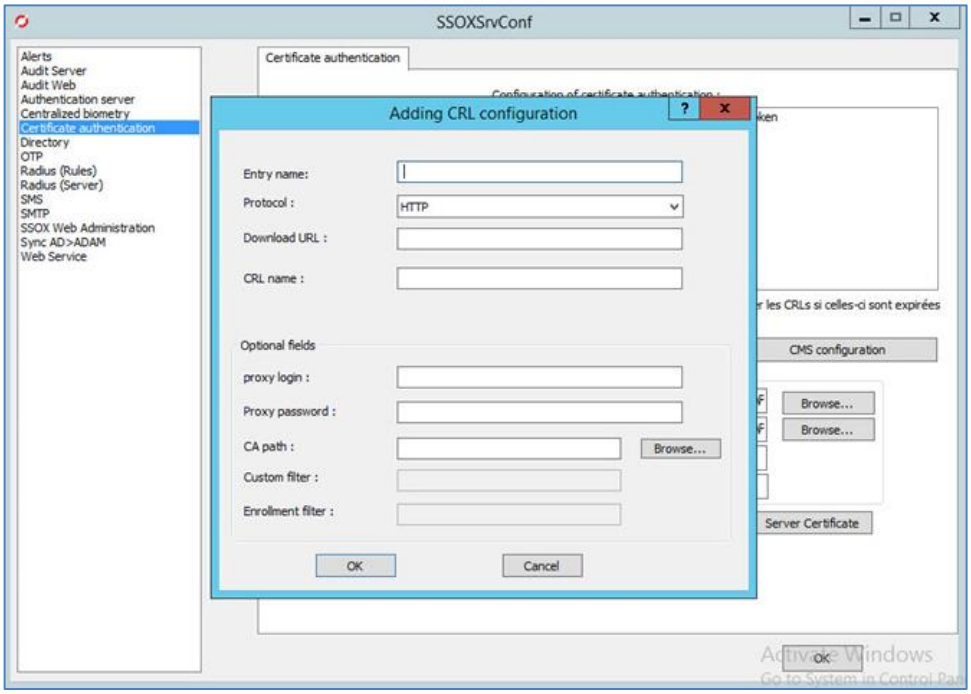
9. After returning to the **SSOXSrvConf** window, under **Manage Certificate**, complete the fields as follows:

Directory containing CAs	Enter the CA path you created in the prerequisites
Directory containing CRLs	Enter the CRL path you created in the prerequisites
Filter of certificate	Enter **(userprincipalname=<cert-cn>)**
Refresh	Keep default value.



10. Under **Configuration of certificate authentication**, click **Add**.

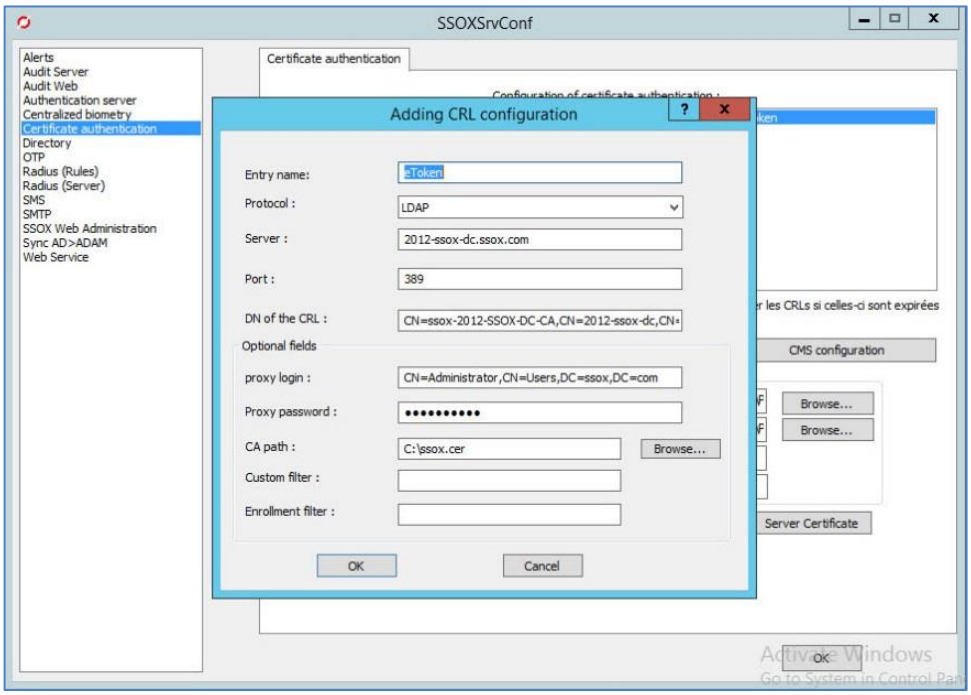
    The **Adding CRL configuration** window opens.



11. Complete the fields as follows:

Entry name	Give a name to the configuration
Protocol	LDAP
Server	Enter the FQDN of the CA server
Port	389
DN of the CRL	Enter the CRL DN
CA Path	Click **Browse** and select the CA certificate
Proxy login	DN of the administrator user

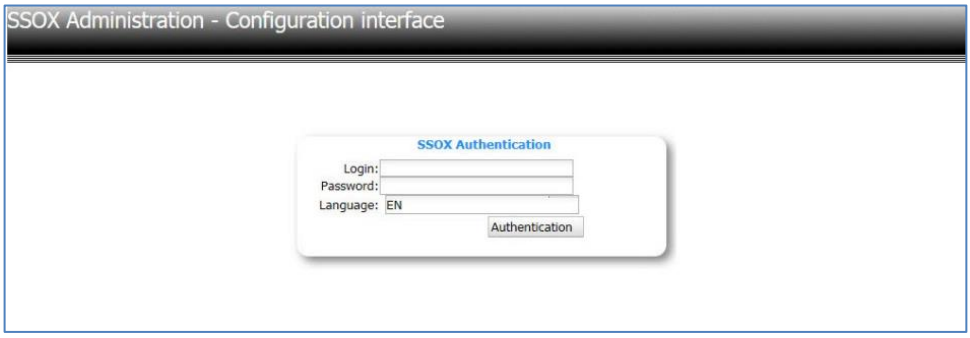
12. Click **OK** to confirm and close the **Adding CRL configuration** window.
13. Click **OK** to confirm and close the **SSOXSrvConf** window**.**



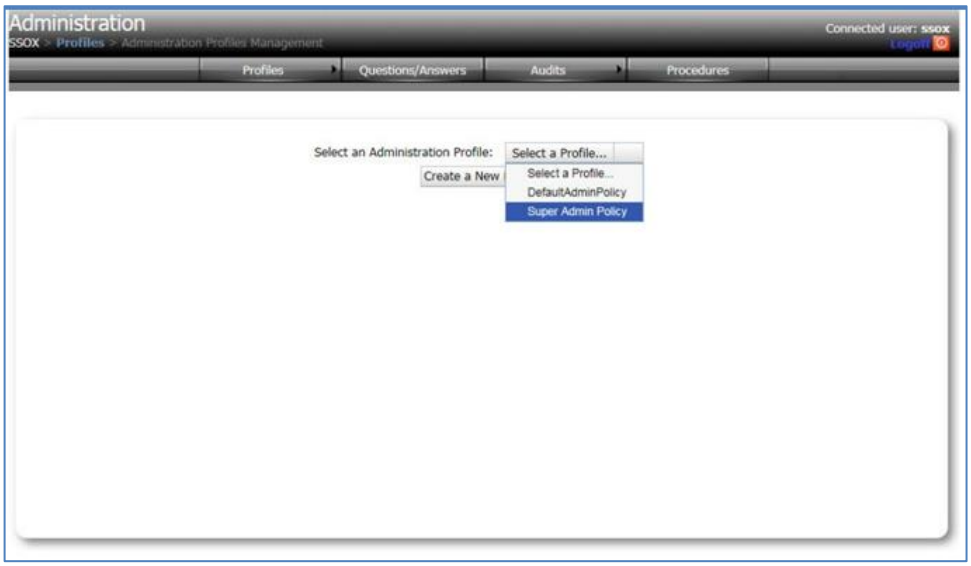
Configure Default Token Template

In this section we will configure the SSOX CMS default template to enroll a new certificate on the smart card/token.

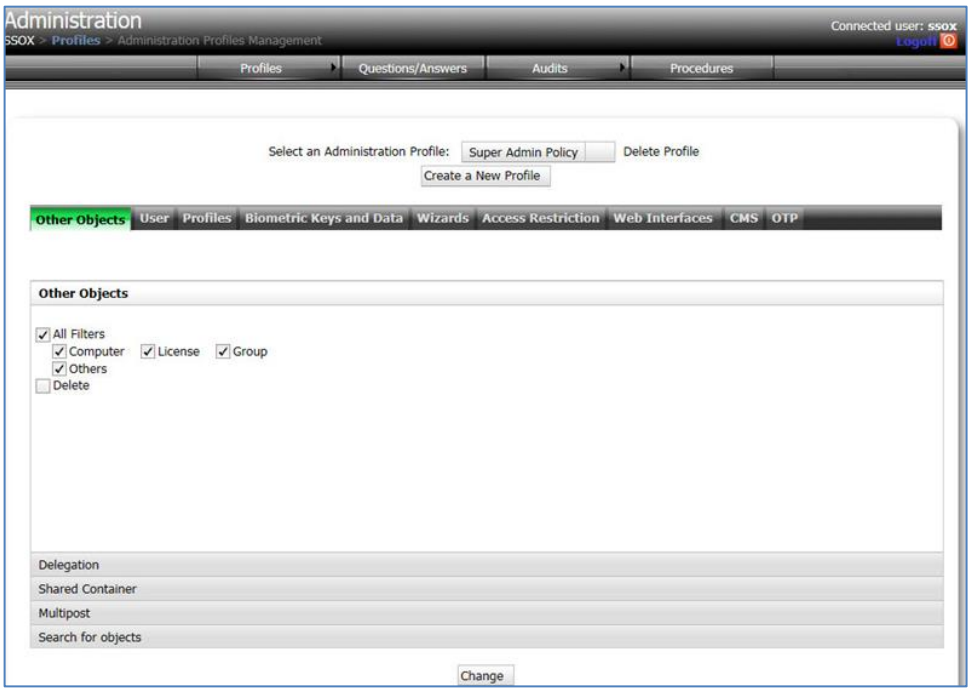
1. Open web browser and go to the SSOX administration configuration page, at: http://<ssox_server>:90/config



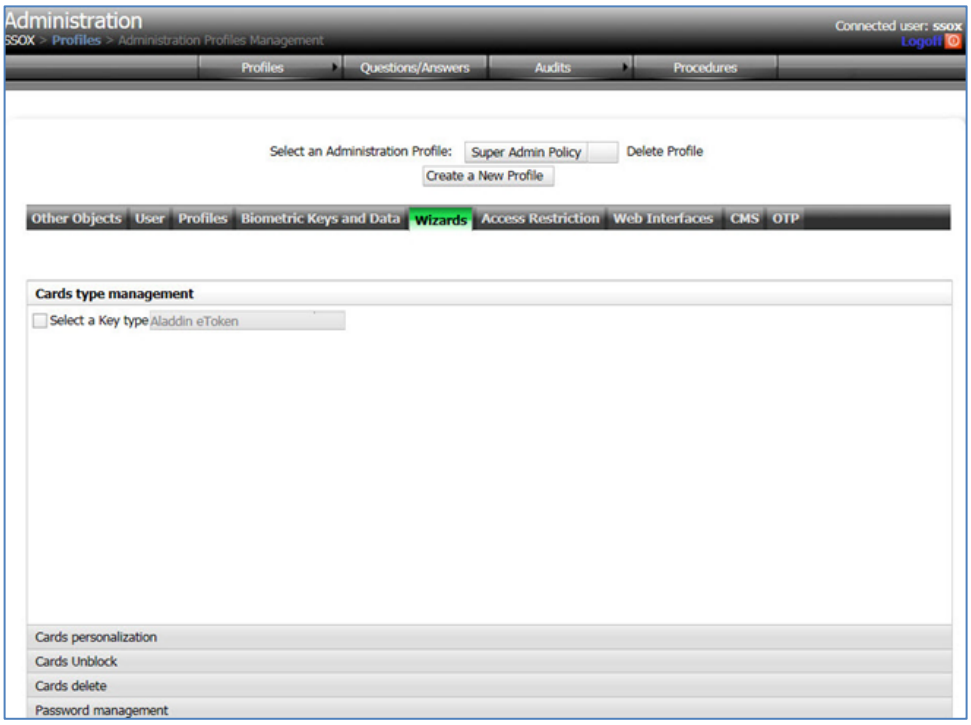
2. After login, click **Select a Profile** and select **Super Admin Policy.**



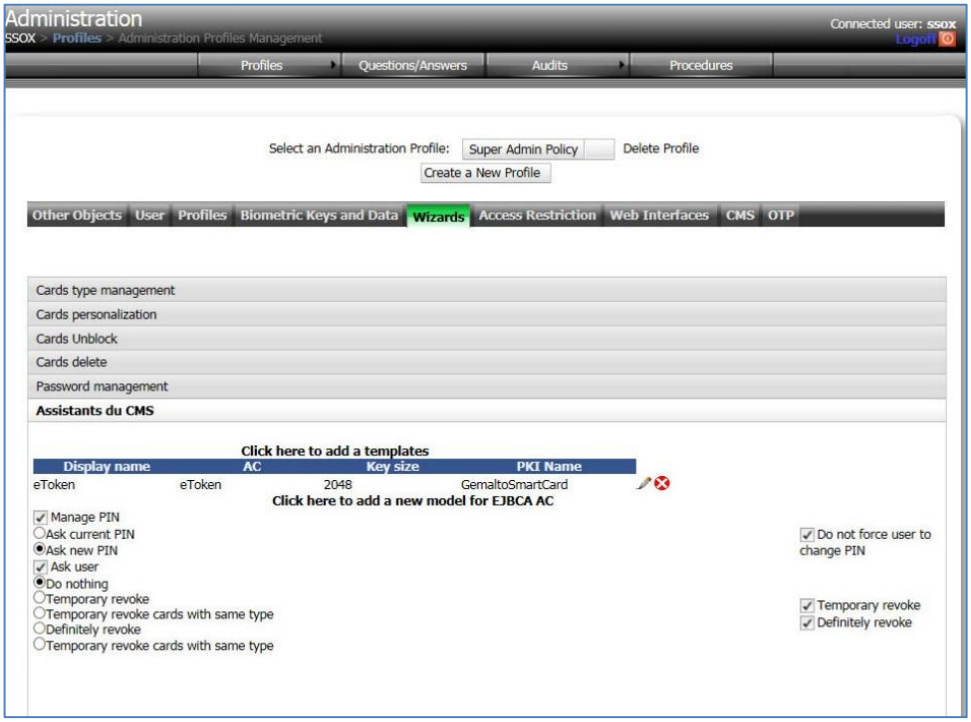
The **Super Admin Policy** window opens



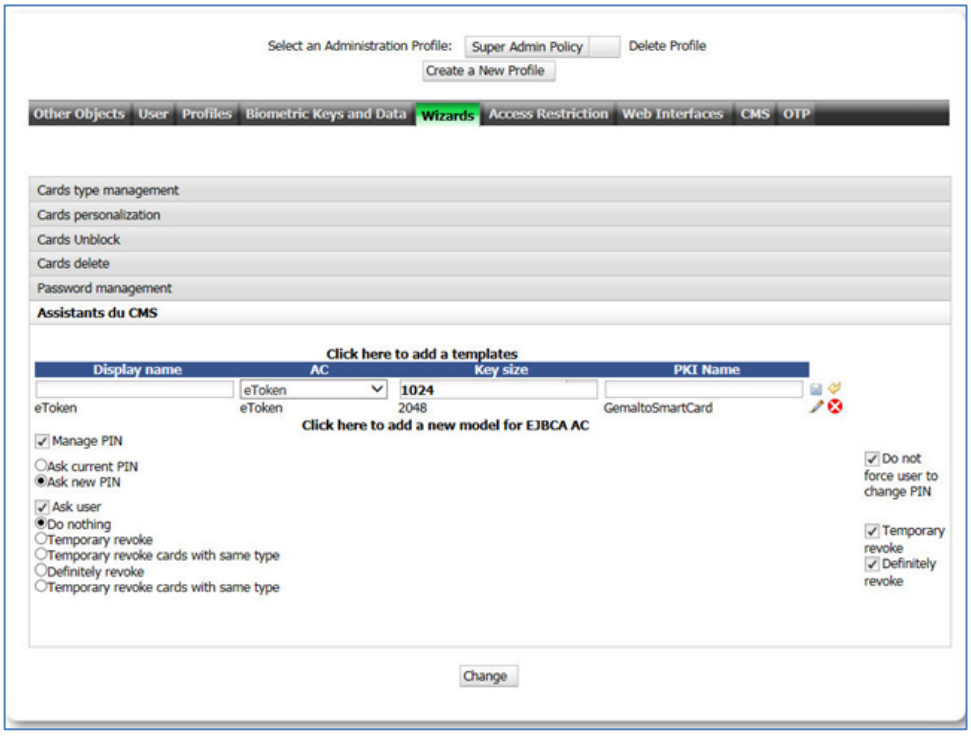
3. Select **Wizards**



4. Select **Assistants du CMS**



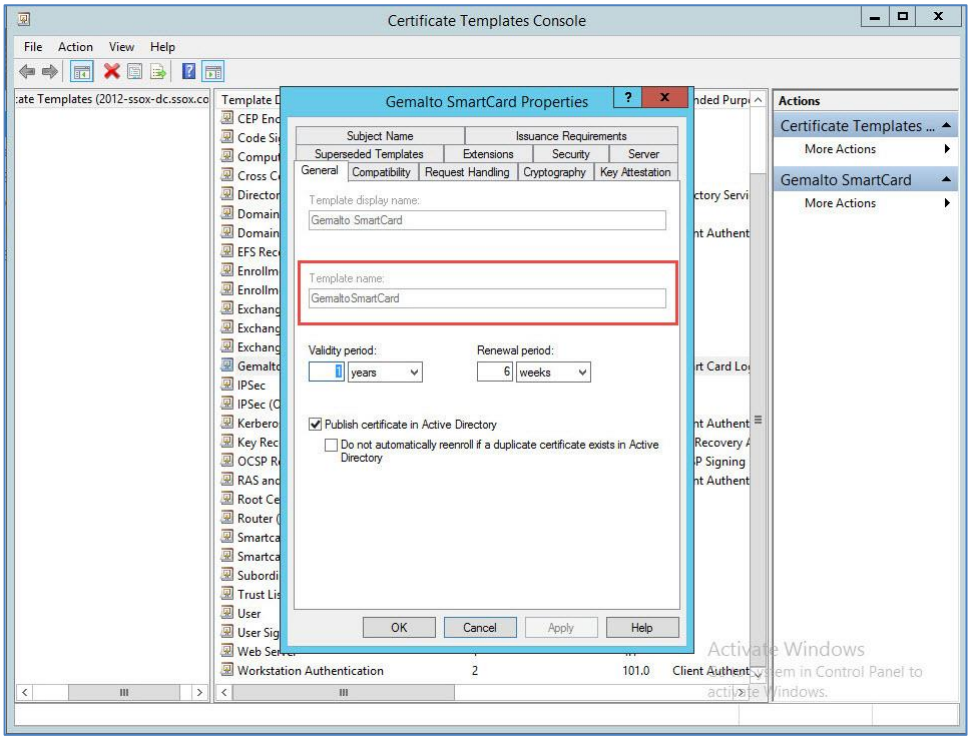
5. Click **Click here to add a template.**



6. Complete the fields as follows:

Display name	Enter a name for the template
AC	Select the PKI template that was created in section "PKI Configuration on SSOX Server" on page 11
Key Size	Select the required key size.
PKI Name	The certificate template name* (which was created in the section "Configuring Certificate Template" on page 10).

* To obtain the template name, go to the **Certificate Templates Console**, in the **Gemalto SmartCard Properties** window, select the **General** tab, and copy the name in the **Template name** field.



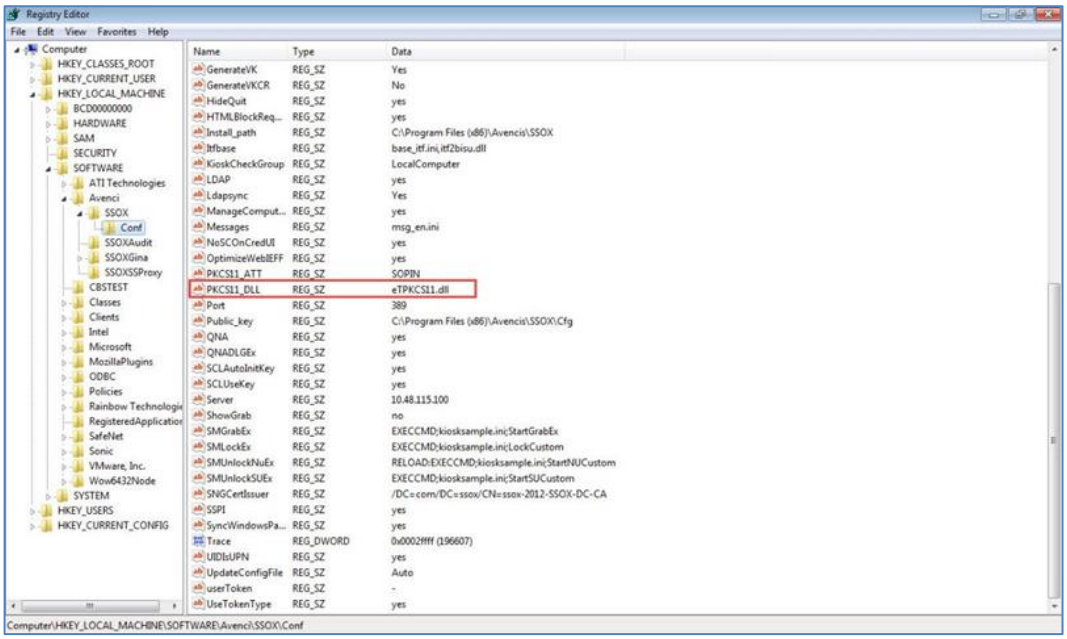
7. Click **Save** and then click **Change**.

Client Configuration: Configure the PKCS#11 path

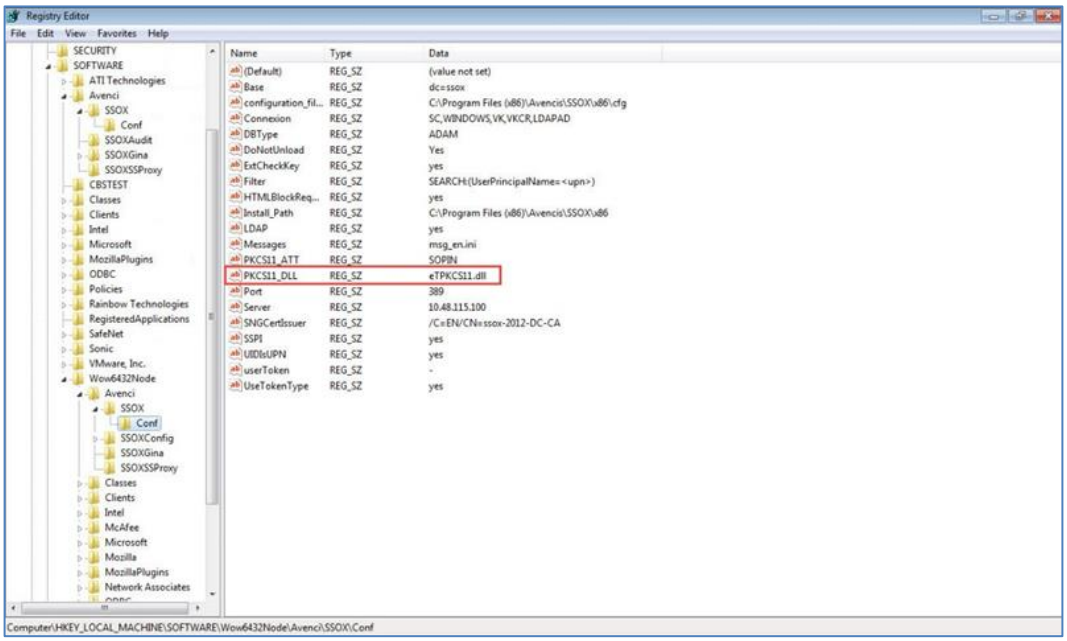
In the following section we will configure SSOX to work with SAC PKCS#11 via the registry file.

On the client machine do the following:

1. Open the **registry** (regedit.exe)
2. Add the following **DWORD32**:
   HKEY_LOCAL_MACHINE\SOFTWARE\Avenci\SSOX\Conf\PKCS11_DLL = eTPKCS11.dll



3. Add the same here:
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Avenci\SSOX\Conf\PKCS11_DLL = eTPKCS11.dll

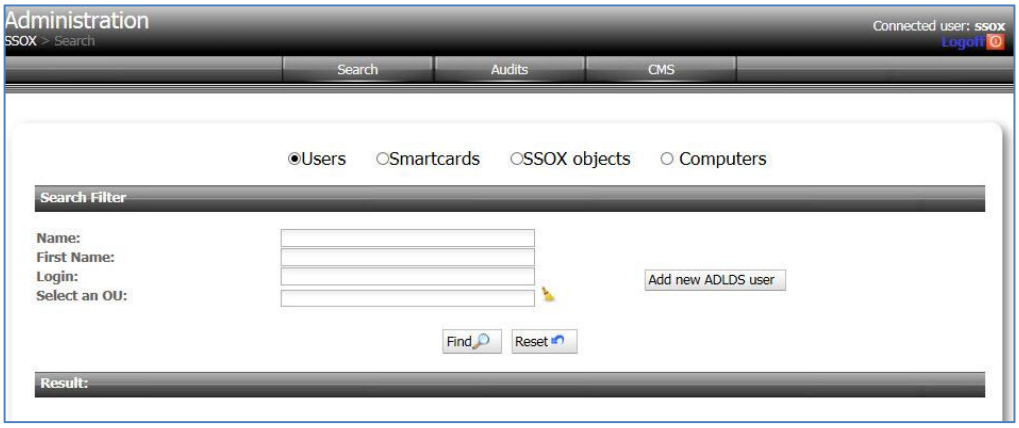


Running the Solution

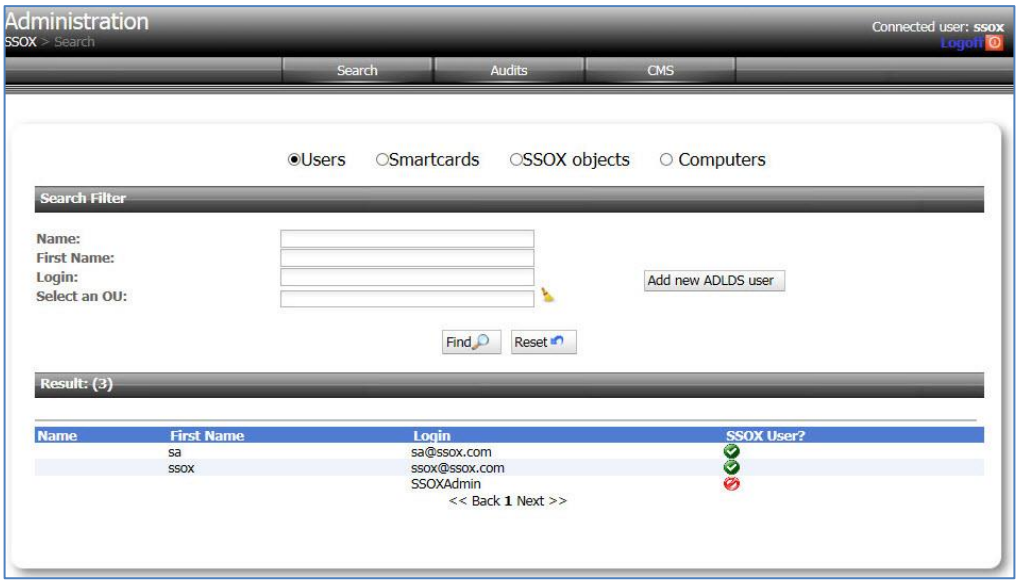
In this section we demonstrate two of the capabilities of Avencis SSOX with SAC.
In this example we use SafeNet eToken 5110 GA.

Enroll a certificate on Token

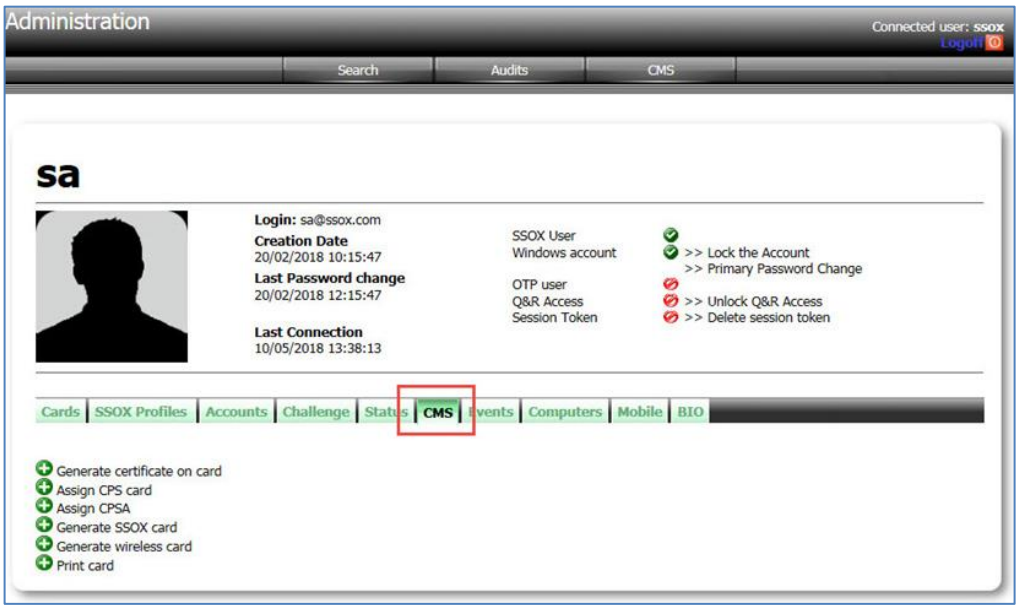
1. Login to the SSOX administration console: http://<ssox_server>:90/config



2. Search for a user.



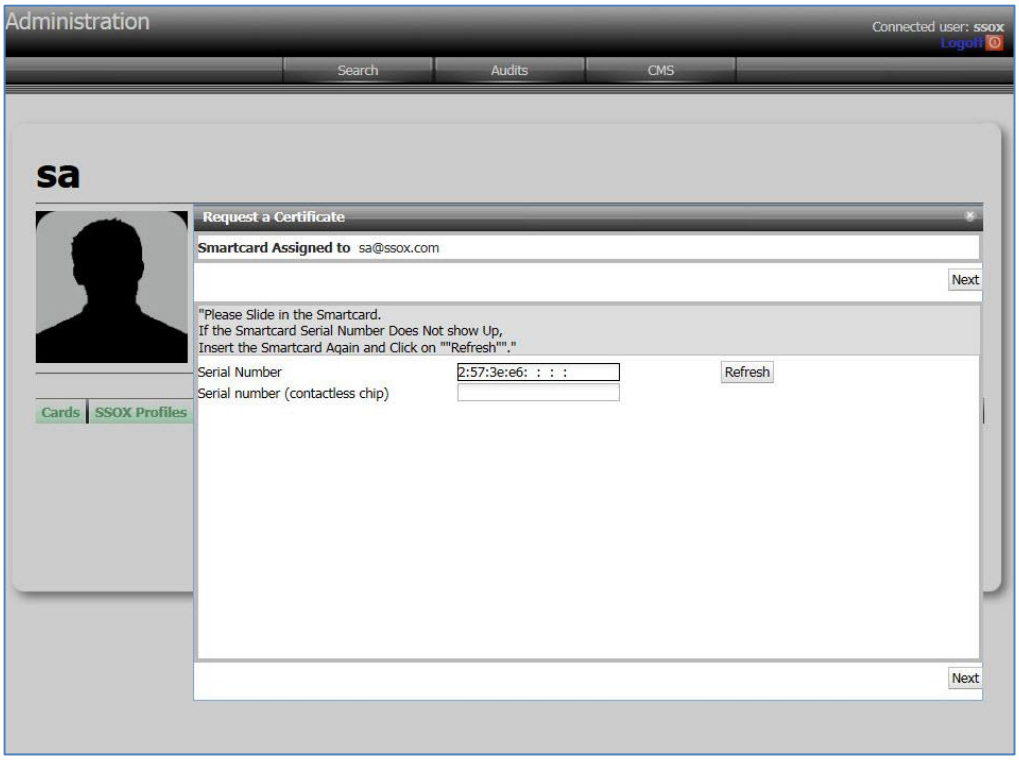
3. Select the relevant user and click **CMS**.



4. Click Generate certificate on card.

   The **Request a Certificate** window opens.

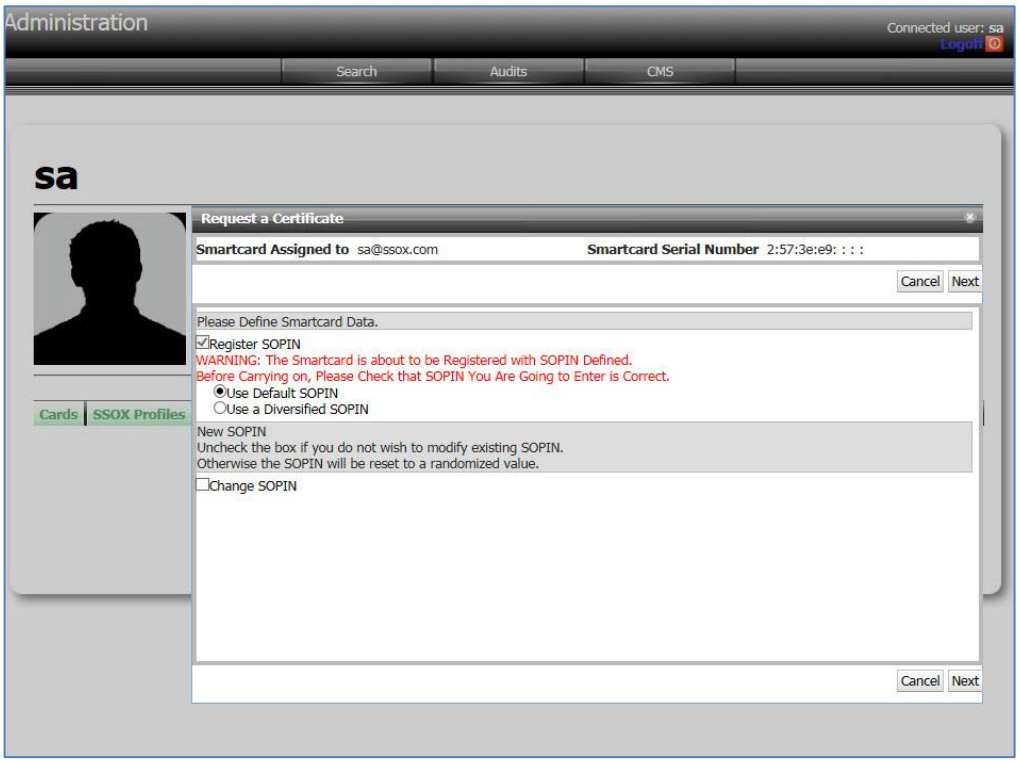
5. If the serial number is not displayed, click **Refresh.**



6. Click **Next**.

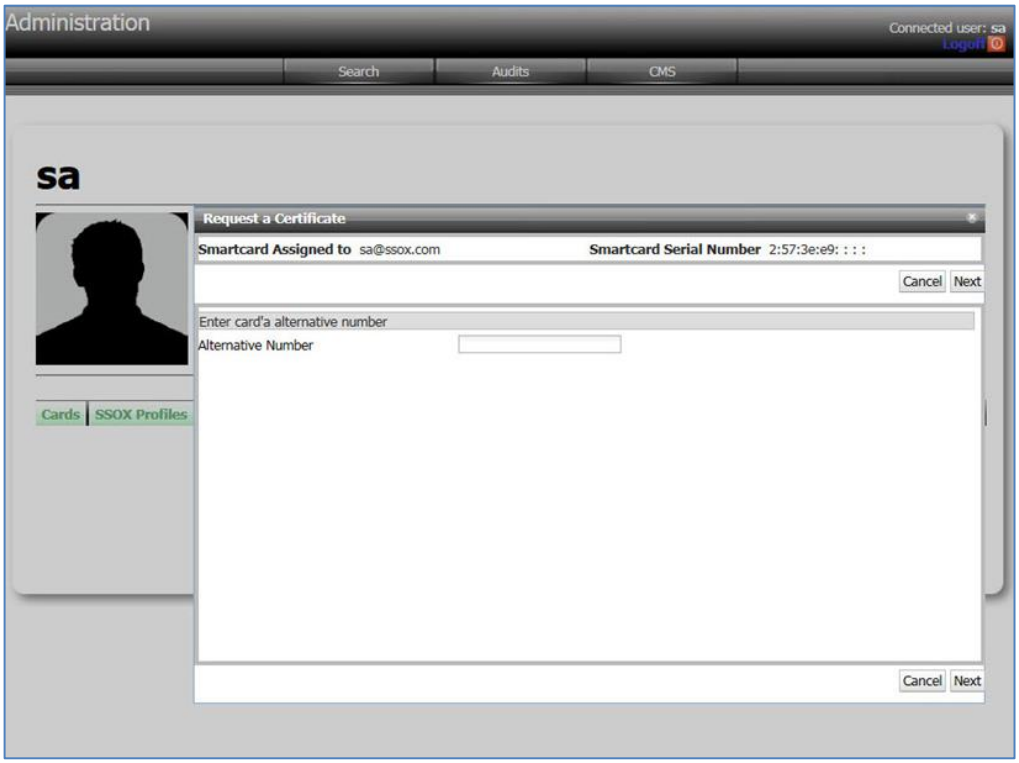
The **Define Smartcard data** window opens (if the token/smartcard is a new OOB token).

7. Select the required configuration and click **Next**.



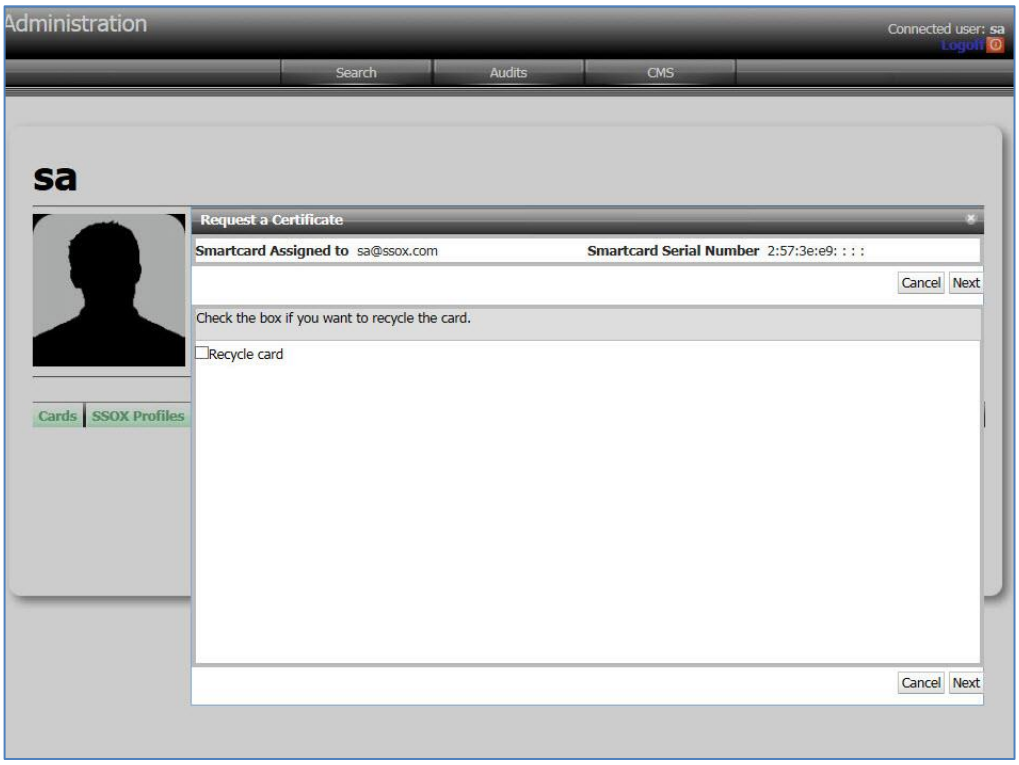
The **Enter card alternative number** is displayed.

8. Select your configuration and click **Next**

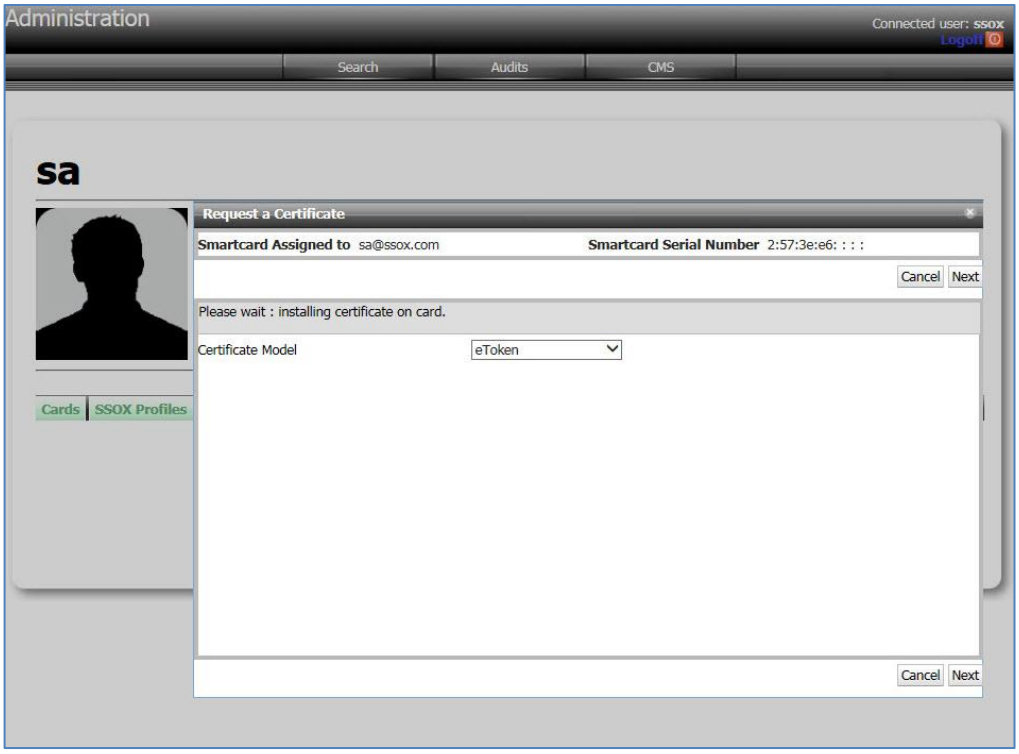


The **Recycle card** window opens.

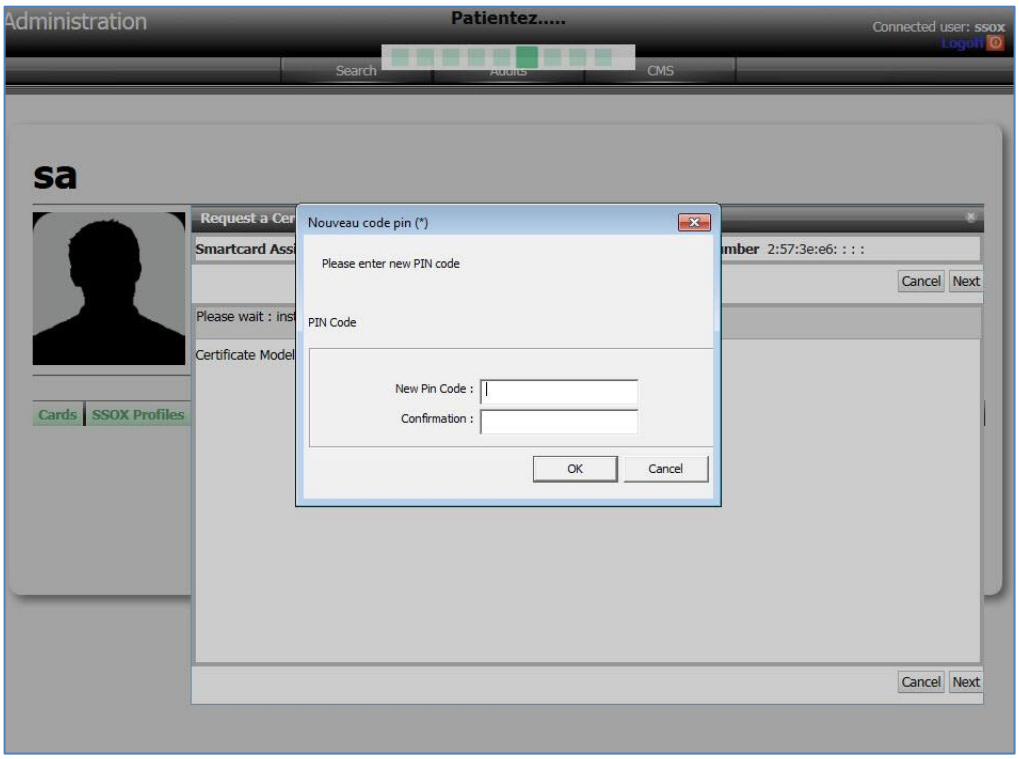
9. Select your configuration and click **Next**.



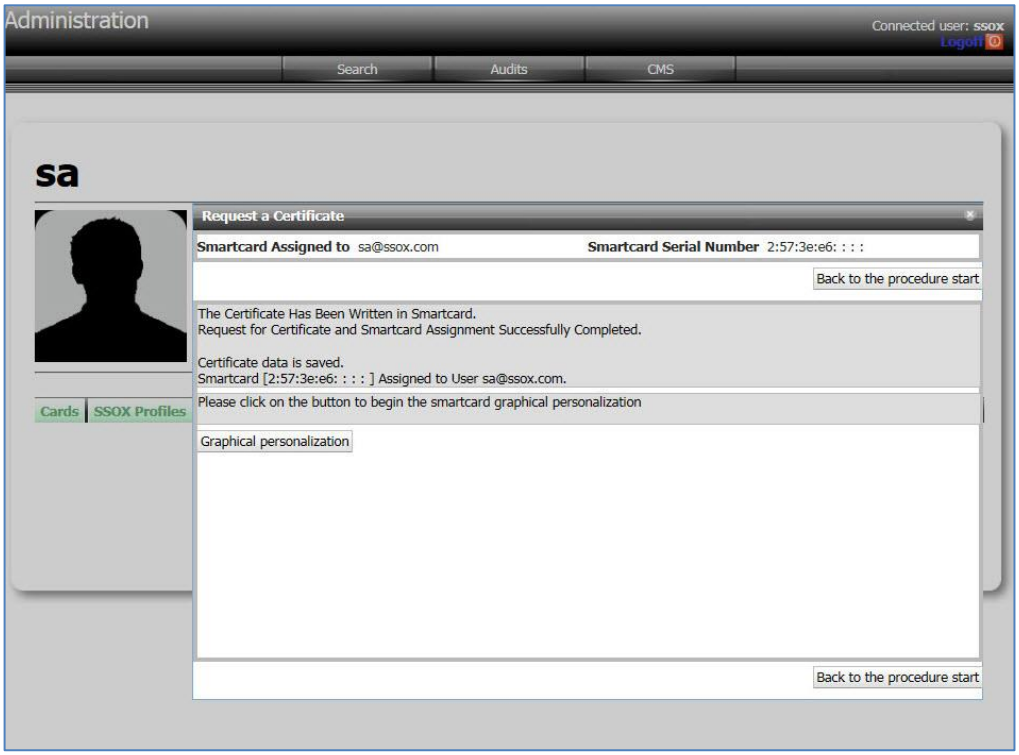
10. Select the **Certificate Model** from the drop-down list and click **Next.**



11. Enter a new PIN code, confirm, and click **OK.**



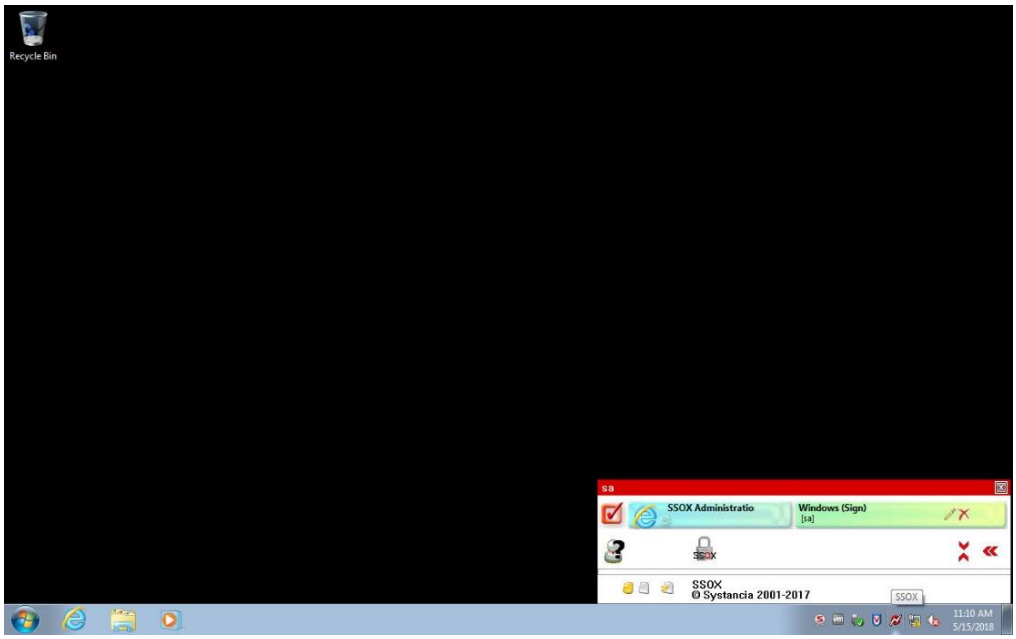
The certificate has been enrolled on the token.



Authenticating to a Web Application

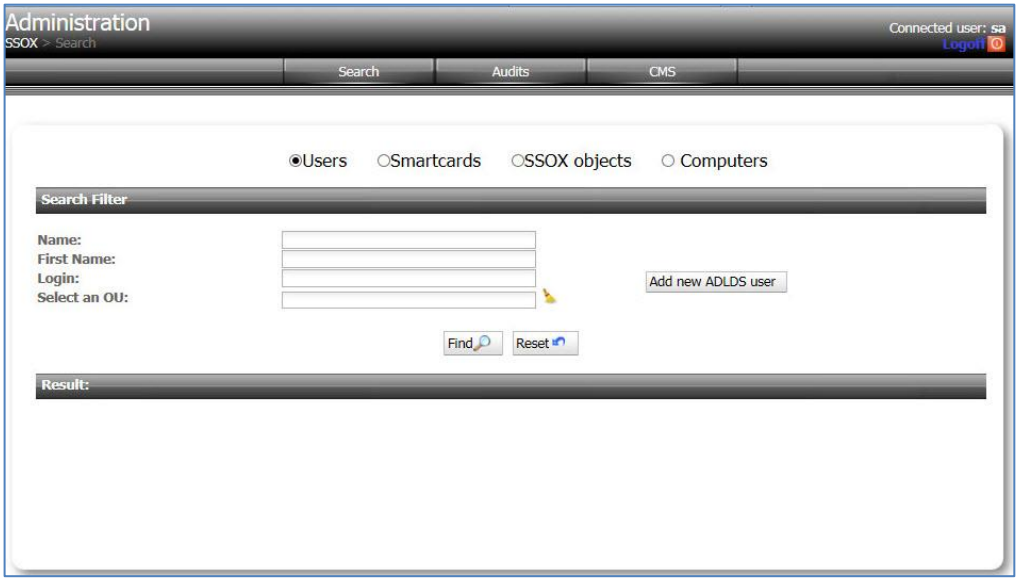
The user performs a **smart card logon** to a Windows 7 machine.

1. When opening the SSOX client the user can select a web application to which he has access.



2. The user clicks the **SSOX Administration** icon.

   The user can now log in to the web application without being required to re-enter the smart card/token PIN code.



Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to 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.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Customer Support by telephone. Calls to Customer Support are handled on a priority basis.

Region	**Telephone number** (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Global	+1-410-931-7520
Australia	1800.020.183
China	North: 10800-713-1971 South: 10800-1301-932
France	0800-912-857
Germany	0800-181-6374
India	000.800.100.4290
Israel	180-931-5798
Italy	800-786-421
Japan	0066 3382 1699
Korea	+82 2 3429 1055

Region	Telephone number (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Netherlands	0800.022.2996
New Zealand	0800.440.359
Portugal	800.863.499
Singapore	800.1302.029
Spain	900.938.717
Sweden	020.791.028
Switzerland	0800.564.849
United Kingdom	0800.056.3158
United States	(800) 545-6608