# SafeNet Authentication Client Integration Guide

Using SafeNet Authentication Client CBA for Avencis SSOX



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.

© 2010 - 2017 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 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 1	0
PKI Configuration on SSOX Server1	1
Configure Default Token Template 1	7
Client Configuration: Configure the PKCS#11 path2	21
Running the Solution 2	22
Enroll a certificate on Token	22
Authenticating to a Web Application 2	27
Support Contacts	28
Customer Support Portal 2	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 certificatebased 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.

SOX Klient Ynstall	
SOX Easy Client Installation upgrade Current Version : 10.0.0.2 ✓ Server is V9 or greater ● EN C F SSOX C AD ● AD/LDS C LDAP First C LDAF	Modules     Image: Constant Con
Directory : 10.48.115.100 Port : >> Base : dc=ssox Authent : 10.48.115.100 Port : Audit : 10.48.115.100 Port :	389     Options       Image: Window on Authen, Failure     Image: Window on Authen, Failure       Image: Window on Authen, Failure     Image: Window on Authen, Failure       Image: Window User to Add Personal App.     Image: Start SSOX at user session startup       Image: Window User to stop SSOX     Image: Start SSOX Cert Renewer       6667     Image: Extended interface     Image: Start VT Emulator Proxy
Authentication Mode C No Device C Bio Central C Bio Local Backup Templates C SmartCard C Wireless Use WL without session C SSQX Container C cond Tures	Manage Pwd Strength IV Display InfoView Show Stop Use Temp Pwd     Bluetooth Connect Don't disable CAD Allow MS Autolog      Filter Cred Prov: V Delete MS SmartCard Cred Prov ation MS SC Logon MS Logon SSOX Logon     MS SC Logon MS Unlock SSOX Logon     MS SC Unlock MS CHOLU SSOX Credui
Certificate Certificate Cert Issuer : //DC=com/DC=ssox/CN □ Test CPS □ Prod CPS ☑ FastCP ☑ Store session token cache 38 □ Support OTP	Kiosk Mode     Login :     Allow Login/Password authentication     Kiosk with no domain     Password :     Display Switch button in inforview     Domain :     Domain :     Lock On Remove Card
I have read the licence     Licence     Licence     Licence     C:\SSOX     C:\SSOX 10.0.0.2\Client Installation\64bir     C:\SSOX 10.0.0.2\Client Installation\64bir     Dire     Command Line     Copy     Cancel	Card To: 100 Mouse To: 50 Mode: Custom vad

<sup>¥</sup> 

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

SOX Klient Ynstall	
SOX Easy Client Installation upgrade Current Version : 10.0.0.2 ✓ Server is V9 or greater ● EN ○ FR ○ CN SSOX ○ AD/LDS ○ LDAP First ○ LDAP Sync	Modules     Image: Circital Provider     Image: HLL API     Image: Circital Analysis     Multistation       Image: Circital Manage: Cir
Directory:         10.48.115.100         Port:         389           >>         Base:         dc=ssox         dc=ssox           Authent:         10.48.115.100         Port:         1777           Audit:         10.48.115.100         Port:         6667	Options           ✓         Hide SSOX Window on Authen. Failure           ✓         Start SSOX a user session startup           ✓         Allow User to Add Personal App.           ✓         Start XCheckNetwork           ✓         Start SSOX Cert Renewer           ✓         Extended interface           ✓         Start VT Emulator Proxy
Authentication Mode C No Device Bio Central C Bio Local E Bio Central C Bio Local S SmartCard C Wireless Use WL without session token SSOX Container C Card Type :	Bluetooth Connect     Don't disable CAD     Allow MS Autolog       Filter Cred Prov :     Image: Delete MS SmartCard Cred Prov       Image: MS SC     Image: MS     SSOX       Image: MS SC Logon     MS Logon     SSOX Logon       Image: MS SC Logon     Image: MS SC Logon     MS Logon       Image: MS SC Logon     Image: MS SC Logon     MS Logon       Image: MS SC Logon     Image: MS SC Logon     MS Logon       Image: MS SC Logon     Image: MS SC Logon     MS Logon       Image: MS SC Logon     Image: MS SC Logon     MS Logon       Image: MS SC Logon     Image: MS SC Logon     SSOX Logon       Image: MS SC Logon     Image: MS SC Logon     SSOX Logon       Image: MS SC Logon     Image: MS SC Logon     SSOX Logon
Certificate <u>Auto     </u> Cert Issuer : /DC=com/DC=ssox/CN=ssox-2     Test CPS     Fod CPS ▼ FastCPS     Store session token cache     3600     Support OTP	Kiosk Mode     Allow Login/Password authentication       Login :     Klosk with no domain       Password :     Display Switch button in infoview       Domain :     Display Operations       Lock On Remove Card
I have read the licence     Licence      SSOX     C:\SSOX 10.0.0.2\Client Installation\64bi     Load     C:\Program Files (x86)\Avencis     Directory      Command Line     Copy     Cancel     Start	Card To: 100 Mouse To: 50 Mode: Custom v

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.

0		SSOXSrvConf	_ <b>_</b> ×
Alerts Audit Server Audit Web Authentication server Centralized biometry Certificate authentication Directory OTP Radius (Rules) Radius (Rules) SMTP SSOX Web Administration Sync AD-ADAM Web Service	Directory Configuration of connec Directory type : Server : Port : Base : user filter : Secrets are stored int	SSOXSrvConf         Directory configuration         ton to directory :         ADAM         127.0.0.1         389         dc=ssox         (UserPrincipalName= <uid>)         o directory.</uid>	
			Activate Windows

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

0	SSOX	SrvConf	
Verts kudit Server kudit Web kuthentication server	Certificate authentication	Configuration of certificate authenticat	tion :
Centralized biometry Certificate authentication Directory	Manage CAs Download protocol :	Add	eToken
TP adius (Rules) adius (Server)	Download URL :	Modify	P
4S 4TP 5OX Web Administration	CRI name :	Delete	n
/mc AD>ADAM /eb Service		Test	
	Proxy login :		e pas vérifier les CRLs si celles-ci sont expiri
	CA :		CMS configuration
	Manage certificate Directory containing CAs :	C:\Program Files (x86)\Avencis\S	SSOX Proxy F Browse
	Directory containing CRLs :	C:\Program Files (x86)\Avencis\S	SSOX Proxy Prowse
	Filter of certificate :	(userprincipalname= <cert-cn>)</cert-cn>	
	Refresh :	86400	
			Server Certificate
			Adtivice W

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

The **CMS options** window opens.

0	SSOXSrvConf	x
Alerts Audit Server Audit Web Authentication server Certificate authentication Directory	Certificate authentication Configuration of certificate authentication : Manage CAs Download protocol : Add	
OTP Radius (Rules) Radius (Server) SMS SMTP SSOX Web Administration	CMS options ? X AC SOPIN automatic renewal Certificate request automatic validation	
Sync AD>ADAM Web Service	CA Type Full name Domain	si celles-ci sont expirées configuration
	Ajouter * Edit Delete Test	owse
	OK Cancel	ertificate
	Adtiv	oke Windows

#### 4. Click Add.

The Add new PKI window opens.

0			SSOXSrvConf			_ 🗆 X
Alerts Audit Server Audit Web Authentication server Centralized biometry Certificate authentication Directory		Certificate aut Manage C Download	Configuratio Configuratio As d protocol :	n of certificate authentication :	eToken	
OTP Radius (Rules) Radius (Server)			CMS options		? X	J
SMS SMTP SSOX Web Administration Sync AD-ADAM Web Service	AC CA Ty Fu Do	Name Type Full name Domain	Add new PKI	OK Cancel		si celles-ci sont expirées configuration wse pwse prtificate
					Adtiv Go to	vake Windows System in Control Pa

Now we will configure the CA.

5. Click Default values.

The Select Certification Authority window opens.

0				SSOXSrvConf			_ 🗆 X
Alerts Audit Server Audit Web Authentication server Centralized biometry		C	ertificate authentication	Configuration of cer	tificate authentication :	eToken	
Directory OTP			Download protocol :	1	Add		
Radius (Rules) Radius (Server)				CMS options		? X	
SMS SMTP SSOX Web Administration	AC		Select (	Certification Authority	? X	×	-
Sync AD>ADAM Web Service	CA	Nam	Select a certification authori	ty (CA) you want to use.			
	Ту	Туре	CA	Computer			
	Ful	Full	STANDALONE-CA	2008r2-ssox.sso	ix.com		si celles-ci sont expirees
	Do	Dom					configuration
						t	pwse
			<	Ш	>	t	pwse
				ОК	Cancel		
			UK	Cancer			
				-			ertificate
		L				Adti	vale Mindows
						Go to	System in Control Par

- 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.

Centralized biometry Cettilizate authentication Prectory TP Sadius (Rules) tadius (Server) MS MTP SOX Web Administration	Manage CAs Download prot	tocol :	Add	eToken	
adius (Rules) adius (Server) MS MTP SOX Web Administration					
MS MTP SOX Web Administration		CMS options		? X	J I
ON WED AUTHING BUDDI		Add new PKI	×		
ic AD SADAM b Service CA Ty Ful Do	Name Type Full name Domain	Gemalto MS CA V 2012-ssox-dc.ssox.com\ssox-2012-SSOX SSOX Default values	-0C-CA		si celles-ci sont expirée: configuration
	L	OK Cance	Cancel		ertificate

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>)</cert-cn>
Refresh	Keep default value.

0	SSOX	SrvConf		×
Alerts Audit Server Audit Web Authentication server Centralized biometry Centralized witherbication Directory OTP Radius (Rules) Radius (Server) SMS	Certificate authentication Manage CAs Download protocol : Download URL :	Configuration of certificate	authentication : Add Modify	
SMTP SSOX Web Administration Sync AD>ADAM Web Service	CRL name :		Test	CRLs si celles-ci sont expirées CMS configuration
	Manage certificate Directory containing CAs :	C:\Program Files (x8	6)\Avencis\SSOX Proxy\F	Browse
	Directory containing CRLs :	C:\Program Files (x8	6)\Avencis\SSOX Proxy\F	Browse
	Filter of certificate :	(userprincipalname= <cert-cn>)</cert-cn>		
	Refresh :	86400		
			Ser	ver Certificate

10. Under Configuration of certificate authentication, click Add.

The Adding CRL configuration window opens.

0	SSOXSrvConf	x
Alerts Audit Server Audit Web	Certificate authentication	
Authentication server Centralized biometry Centralized biometry Directory OTP Radius (Rules) Radius (Rules) Radius (Rules) SMTP SSOT Web Administration Sync AD-ADAM Web Service	Configuration of cartificate authenticate       Adding CRL configuration       Entry name:       Protocol :       HTTP       v       Download URL :       CRL name :       Optional fields       proxy login :       Proxy password :       CA path :       Custom filter :       Enrolment filter :	x ken r les CRLs si celles-ci sont expirées CMS configuration F Browse F Browse Server Certificate

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.

2		SSOXSrvConf		>
Alerts Audit Server Audit Web	Certificate authent	ication		
Authentication server Centralized biometry Certificate authentication		Adding CRL configuration	? X	ken
Directory DTP Radius (Rules) Radius (Server)	Entry name:	eToken		
MS MTP	Protocol :	LDAP	~	
SUX web Administration ync AD>ADAM leb Service	Server :	2012-ssox-dc.ssox.com		
	Port :	389		
	DN of the CRL :	CN=ssox-2012-SSOX-DC-CA,CN=2012-ssox	(-dc,CN=	r les CRLs si celles-ci sont expirée
	Optional fields	7		CMS configuration
	proxy login :	CN=Administrator,CN=Users,DC=ssox,DC=	com	F
	Proxy password :			F Browse
	CA path :	C:\ssox.cer	Browse	
	Enrollment filter :			
				Server Certificate
	ОК	Cancel		
				Lai
				Adtivioke Windows

## **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

Login: Password: Language:	SSOX Authentication
	Authentication

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

ministration x > Profiles > Administration	Profiles Managem	ent.			Connected user: sse
	Profiles	Questions/Answers	Audits	Procedures	
		Select an Administration Profile:	Select a Profile		
		Create a New	Select a Profile		
			DefaultAdminPolicy Super Admin Policy		
		2	Super Autim Policy		

#### The Super Admin Policy window opens

TITTISUCATION > Profiles > Administration P	rofiles Management				Connected user: : Logo
	Profiles	Questions/Answers	Audits	Procedures	
	Select an Adm	ninistration Profile: Sup Create a Ne	er Admin Policy w Profile	Delete Profile	
Other Objects User Prof	les Biometric Keys	and Data Wizards A	ccess Restriction	Web Interfaces CMS	ОТР
Other Objects					
All Filters     Computer     Computer     Others     Delete	Group				
Delegation					
Delegation Shared Container					
Delegation Shared Container Multipost					

#### 3. Select Wizards

ministration X > Profiles > Administration Pr	ofiles Managem	ent			Connected user: ss
	Profiles	Questions/Answe	rs Audits	Procedures	
	Select	an Administration Profile:	Super Admin Policy	Delete Profile	
		Creat	e a wew Prome		
Other Objects User Profile	s Biometric	Keys and Data Wizard	Access Restricti	on Web Interfaces CMS	б отр
Carde time management					
Caros type management					
Cards personalization					
Cards delete					
Paceword management					

#### 4. Select Assistants du CMS

ninistratio > Profiles > Ad	n Iministration Profile	is Manageme	ent.			Connected user: ss
_		Profiles	Questions/Ans	wers Audits	Procedures	
		Select	an Administration Profile	e: Super Admin Policy	/ Delete Profile	
			Cre	eate a New Profile		
Other Objects	User Profiles	Biometric	Keys and Data	ards Access Restrict	tion Web Interfaces Cl	IS OTP
					and a second data and second and	
Cards type mana	gement					
Cards personaliza	ation					
Cards Unblock						
Cards delete						
Password manag	ement					
Assistants du C	MS					
		Click here	to add a templates			
Display na	me oTokon	AC	Key size	PKI Nam	e	
eroken	eroken	Click	here to add a new m	odel for EJBCA AC		
Manage PIN						
OAsk current PIN	4					Do not force user to
SASK new PIN						change PIN
Ask user						
Temporary rev	oke					
Temporary revo	oke cards with sam	e type				✓ Temporary revoke
Definitely revok	æ					Pennitely revoke
JTemporary revo	oke cards with sam	ie type				

5. Click Click here to add a template.

	Select an A	dministration Profile:	Super Admin Policy	Delete Profile	
		Create	e a New Profile		
Other Objects User Profi Cards type management Cards personalization Cards Unblock Cards delete Password management Assistants du CMS	iles Biometric Key	rs and Data Wizar	ds Access Restrictio	n Web Interfaces CMS O	TP
Dicelay name		lick here to add a t	emplates Kou sizo	DVT Name	_
Unspilay name	eToken	✓ 1024	Ney Size	PRINdille	
eToken	eToken	2048		GemaltoSmartCard	10
✓ Manage PIN	Click	here to add a new	model for EJBCA AC		
OAsk current PIN					✓ Do not force user to change PIN
Ask new PIN Ask user Do nothing Temporary revoke Temporary revoke Cefinitely revoke Temporary revoke cards with Temporary revoke cards with	h same type h same type				✓ Tempora revoke ✓ Definitely revoke

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.

Templates (2012-ssox-dc.ssox.co Tem	plate D	Gemal	to SmartCard	Properties	? X	nded Purp	Actions
2 C	EP End	Cubinat Name	1				Certificate Template
	omput Supe	seded Templates	Extensions	Security	Server		More Actions
	ross C General	Compatibility F	Request Handling	Cryptography	Key Attestation		Complete EmpetCord
	irector Tomo	to display name:				ctory Servi	Gernario Smaricaru
	omain Gema	to SmartCard					More Actions
	omain	to Smarteard				nt Authent	
2 E	FS Rec						
R E	nrollm Templ	ate name:					
e e	Gema	to SmartCard					
(2) E	xchang						
 	xchang	100000000000000000000000000000000000000		and a second			
	iemalto	penod:	Kenewa	penod:		rt Card Loi	
91 💭	Sec	years V	ь	weeks 🗸			
31 🖳	Sec (C						
🗵 к	erbero 🖌 Pul	olish certificate in A	ctive Directory			nt Authent ≡	
Ш к	ey Rec	Do not automatical	lly reenroll if a duplic	ate certificate e	xists in Active	Recovery A	
	CSP R	Directory				P Signing	
R R	AS and					nt Authent	
R R	oot Ce						
CHER R	outer (						
ा । ज	martca						
R s	ubordi						
I T	rust Lis						
	lser						
2 U	lser Sig	ОК	Cancel	Apply	Help		
	Veb Server		10			Activat	e Windows

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

Registry Editor				×
ile Edit View Favorites Help				
Computer	Name	Туре	Data	
HKEY_CLASSES_ROOT	GenerateVK	REG_SZ	Yes	
HKEY_CURRENT_USER	GenerateVKCR	REG_SZ	No	
A HKEY_LOCAL_MACHINE	HideQuit	REG SZ	ves	
BCD0000000	HTMLBlockReg.	REG_SZ	ves	
	a Install path	REG SZ	C/\Program Files (x86)\Avencis\SSQX	
D - SAM	a) Itfbase	REG SZ	base infini inf2bisu.dll	
SOETWARE	MioskCheckGroup	REG_SZ	LocalComputer	
ATI Technologies	- LDAP	REG SZ	ves	
Aunci	A Ldapsync	REG SZ	Yes	
SSOX	ManageComput	REG SZ	ves	
Cont	Messages	REG SZ	msa enini	
SSOXAudit	MoSCOnCredUI	REG SZ	ves	
> - E SSOXGina	A OptimizeWeblEFF	REG SZ	ves	
SSOXSSProxy	A PKCS11 ATT	REG SZ	SOPIN	
CBSTEST	PKCS11 DLL	REG SZ	eTPKCS11.dll	- 8
b - L Classes	A Port	REG SZ	389	
> 🍶 Clients	Public key	REG SZ	C:\Program Files (x86)\Avencis\SS0X\Cfg	
s 🕌 Intel	A QNA	REG SZ	ves	
⊨ Microsoft	MADLGEx	REG_SZ	yes	
MozillaPlugins	M SCLAutoInitKey	REG SZ	ves	
DOBC	M SCLUseKey	REG SZ	ves	
Policies	A Server	REG SZ	10.48.115.100	
Alinbow Technologie	A ShowGrab	REG_SZ	no	
RegisteredApplication	MGrabEx	REG SZ	EXECCMD:kiosksample.ini:StartGrabEx	
Serves	MLockEx	REG SZ	EXECCMD:kiosksample.ini:LockCustom	1
Vitimere Inc.	MUnlockNuEx	REG_SZ	RELOAD:EXECCMD:kiosksample.ini;StartNUCustom	
Wow6432Node	MUnlockSUEx	REG_SZ	EXECCMD:kiosksample.ini;StartSUCustom	
SYSTEM	M SNGCertIssuer	REG_SZ	/DC=com/DC=ssox/CN=ssox-2012-SSOX-DC-CA	
HKEY USERS	e SSPI	REG_SZ	yes	
HKEY_CURRENT_CONFIG	SyncWindowsPa	REG_SZ	yes	
-	Trace	REG_DWORD	0x0002899 (196607)	
	UIDILUPN	REG_SZ	yes	
	A UpdateConfigFile	REG_SZ	Auto	
	euserToken	REG_SZ		
1 10 1	M UseTokenType	REG SZ	ves	1

3. Add the same here: HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Avenci\SSOX\Conf\PKCS11\_DLL = eTPKCS11.dll

SafeNet Authentication Client: Integration Guide Using SafeNet Authentication Client CBA for Avencis SSOX Document PN: 007-000153-001, Rev. A

# **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

Iministration x > Search				Connected user: sso
	Search	Audits	CMS	
Search Filter	⊛Users OSi	martcards OSSOX objec	cts O Computers	
Name: First Name: Login: Select an OU:			Add new ADLDS user	
Result:		Find Reset 🖍		

2. Search for a user.

dministration DX > Search					Connected user: sso
		Search	Audits	CMS	
		OSma	rtcards OSSOX obje	ects O Computers	
Search Filter	_				
Name:					
First Name:					
Login:				Add new ADLDS user	
Select an OU:					
			Find P Reset 🗖		
Result: (3)	_				
Name	First Name	- 10	ogin	SSOX User?	
	sa	sa	@ssox.com	<b>2</b>	
	SSOX	SS	ox@ssox.com	0	
		55	OXAdmin	6	
			SS DOCK I NOAL ??		

3. Select the relevant user and click CMS.

nistration				Connected us
	Search	Audits	CMS	
3				
1	Login: sa⊕ssox.com Creation Date 20/02/2018 10:15:47 Last Password change 20/02/2018 12:15:47 Last Connection 10/05/2018 13:38:13	SSOX User Windows account OTP user Q&R Access Session Token	<ul> <li>&gt;&gt; Lock the Account</li> <li>&gt;&gt; Primary Password Change</li> <li>&gt;&gt; Unlock Q&amp;R Access</li> <li>&gt;&gt; Delete session token</li> </ul>	1
ds SSOX Profiles Ac	counts Challenge Status CM	Is I vents Computers Mo	BIO	_
ssign CPS card ssign CPSA enerate SSOX card enerate wireless card int card				

4. Click Generate certificate on card.

The Request a Certificate window opens.

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

a				
	Request a Certificate			
	Smartcard Assigned to sa@ssox	com		
	"Please Slide in the Smartcard. If the Smartcard Serial Number Doe Insert the Smartcard Aqain and Clic	es Not show Up, k on ""Refresh""."		
ards SSOX Prof	Serial Number Serial number (contactless chip)	<u>2:57:3e:e6: : : :</u>	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.

ministration				C	onnected	d user
	Search	Audits	CMS	_		
sa						
	Request a Certificate		_		_	*
	Smartcard Assigned to sa@ssox.com		Smartcard Serial Num	ber 2:57:3e:e9: : : :		
					Cancel	Nex
	Please Define Smartcard Data.					
Cards SSOX Profiles	Register SOPIN WARNING: The Smartcard is about to be R Before Carrying on, Please Check that SOP ©Use Default SOPIN OUse a Diversified SOPIN	Registered with SOPIN IN You Are Going to E	Defined. inter is Correct.			
	New SOPIN Uncheck the box if you do not wish to mod Otherwise the SOPIN will be reset to a ran	dify existing SOPIN. domized value.				
	Change SOPIN					
	L				Cancel	Nex

The Enter card alternative number is displayed.

8. Select your configuration and click Next

				Conhected
	Search	Audits	CMS	_
a				
	Request a Certificate	_		
	Smartcard Assigned to sa@sso:	x.com	Smartcard Serial Number 2:	7:3e:e9: : : :
				Cancel 1
	Enter card'a alternative number			
	Alternative Number			
	-			
ards SSOX Profile	5			
				Cancel
				Cancer

The Recycle card window opens.

9. Select your configuration and click Next.

istration		_	Connected
	Search A	udits CMS	
_			
a			
	Request a Certificate	_	
	Smartcard Assigned to sa@ssox.com	Smartcard Serial Num	ber 2:57:3e:e9: : : :
			Cancel
	Check the box if you want to recycle the card.		
	Recycle card		
ds SSOX Profiles			
	1		
			Cancel

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

	Convolu	Audito	640			Log
	Search	Audits	CMS			
a						
	Request a Certificate	-		-	_	
	Smartcard Assigned to sa@ssox.com		Smartcard Serial Numb	er 2:57:3e:e6: : : :		
					Cancel	N
	Please wait : installing certificate on card.					
	Certificate Model	eToken	~			
		174				
ards SSOX Profiles						
	1					
					Cancel	N
						_

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

Administration	Patientez	Connected user: ssox
	Search Audics CMS	Logott 🧕
Sa Regu Smart Please Certific	Lest a Cer     Nouveau code pin (*)       Image: Carcel Assister of the second s	3e:e6: : : : Cancel Next
		Cancel Next

The certificate has been enrolled on the token.

Sa Reques Smartca The Cert Request Certificat Smartca Smartca Smartca Smartca Smartca Cards SSOX Profiles	Search at a Certificate ard Assigned to sa@ssox.com ificate Has Been Written in Smartcard. for Certificate and Smartcard Assignment the data is saved. rd [2:57:3e:e6: : : : ] Assigned to User s ick on the button to begin the smartcard	Audits Sm nt Successfully Comp sa@ssox.com. d graphical personali	CMS nartcard Serial Nun	nber 2:57:3e:e6: : : : Back to the procedure sta
Sa Reques Smartca The Certificat Cards SSOX Profiles Cards SSOX Profiles	at a Certificate and Assigned to sa@ssox.com ificate Has Been Written in Smartcard. for Certificate and Smartcard Assignmer te data is saved. Id [2:57:3e:e6: : : : ] Assigned to User s ick on the button to begin the smartcard	Sm nt Successfully Comp sa@ssox.com. d graphical personali	aartcard Serial Nun eleted.	nber [2:57:3e:e6: : : : Back to the procedure sta
Cards SSOX Profiles Request Certificat Smartca	it a Certificate and Assigned to sa@ssox.com ificate Has Been Written in Smartcard. for Certificate and Smartcard Assignment re data is saved. rd [2:57:3e:e6: : : : ] Assigned to User s ick on the button to begin the smartcard	Sm nt Successfully Comp sa@ssox.com. d graphical personali	nartcard Serial Nun	nber 2:57:3e:e6: : : : Back to the procedure sta
Cards SSOX Profiles Smartca	and Assigned to sa@ssox.com ificate Has Been Written in Smartcard. for Certificate and Smartcard Assignment te data is saved. Id [2:57:3e:e6: : : : ] Assigned to User s ick on the button to begin the smartcard	Sm nt Successfully Comp sa@ssox.com. d graphical personali	nartcard Serial Nun	nber 2:57:3e:e6: : : : Back to the procedure sta
Cards SSOX Profiles	ificate Has Been Written in Smartcard. for Certificate and Smartcard Assignmer re data is saved. Id [2:57:3e:e6: : : : ] Assigned to User s ick on the button to begin the smartcard	nt Successfully Comp sa@ssox.com. d graphical personali	leted.	Back to the procedure sta
Cards SSOX Profiles Graphica	ificate Has Been Written in Smartcard. for Certificate and Smartcard Assignmen te data is saved. Id [2:57:3e:e6: : : ] Assigned to User s ick on the button to begin the smartcard	nt Successfully Comp sa@ssox.com. d graphical personali	leted.	
Graphica		a graphear personan	zation	
	al personalization			
				Back to the procedure sta

## 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.

8					 _	 	_	_					
Recycle Bi	n												
								sa	S 550	OX Administratio	Windows (Sign)		
									30	0	[53]	1	
								8		SISOX			× «
								08	1	SSOX © Systancia 2001	-2017	SSOX	
<b>1</b>	8	ien.	0								یا 🖻 😒	💟 💋 🛐 🌜	11:10 AM 5/15/2018

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.

dministration 50X > Search		-		Connected user: sa
	Search	Audits	CMS	
Search Filter	©Users ○Smar	tcards OSSOX obje	ects O Computers	
Name: First Name: Login: Select an OU:			Add new ADLDS user	
		Find Reset 🔊		
Result:		_		_

# **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	<b>Telephone number</b> (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