# SafeNet Authentication Client Integration Guide

Using SafeNet Authentication Client CBA for Citrix NetScaler Access Gateway



All information herein is either public information or is the property of and owned solely by Gemalto NV. 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.

© 2016 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 Part Number: 007-013480-001, Rev. A Release Date: August 2016

# Contents

Third-Party Software Acknowledgement
Description
Applicability
Environment
Audience
CBA Flow using SafeNet Authentication Client
Prerequisites
Supported Tokens in SafeNet Authentication Client
Configuring Citrix NetScaler Access Gateway7
Configuring Citrix StoreFront
Configuring SmartCard Pass-through12
Running the Solution
Using SAC CBA for Citrix Web Access13
Using SAC CBA for Citrix Receiver Application Access14
Using SAC CBA with SSO for Citrix Web Access16
Using SAC CBA with SSO for Citrix Receiver Application Access16
Appendix: Modifying the CSP PIN Prompt from Citrix Default to SafeNet Authentication Client
Support Contacts

## **Third-Party Software Acknowledgement**

This document is intended to help users of Gemalto products when working with third-party software, such as Citrix NetScaler Access Gateway.

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**

Customers today are looking to desktop virtualization to transform static desktops into dynamic mobile workspaces that can be centrally and securely managed from the datacenter, and accessed across a wide range of devices and locations. Deploying desktop virtualization 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.

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. SafeNet's certificate-based tokens 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.

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 life cycle. 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.

SAM is a comprehensive token management system. It is an out-of-the-box solution for Public Certificate Authorities (CA) and enterprises to ease the administration of SafeNet's hardware or software tokens devices. SAM is designed and developed based on the best practices of managing PKI devices in common PKI implementations. It offers robust yet easy to customize frameworks that meets different organizations' PKI devices management workflows and policies. Using SAM to manage tokens is not mandatory, but it is recommended for enterprise organizations.

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

Citrix NetScaler Access Gateway is a secure application and data access solution that gives IT administrators a single point to manage access control and limit actions within sessions based on both user identity and the endpoint device. New threats, risks, and vulnerabilities as well as evolving business requirements underscore to the need for a strong authentication approach based on multi-factor authentication.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Citrix NetScaler Access Gateway using SafeNet tokens.

SafeNet Authentication Client: Integration Guide Using SafeNet Authentication Client CBA for Citrix NetScaler Access Gateway Document PN: 007-013480-001, Rev. A, © Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries. It is assumed that the Citrix NetScaler Access Gateway environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

Citrix NetScaler Access Gateway can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with SafeNet products.

## Applicability

The information in this document applies to:

- SafeNet Authentication Client (SAC)—SafeNet Authentication Client is the middleware that manages SafeNet's tokens.
- Citrix NetScaler Access Gateway

### **Environment**

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

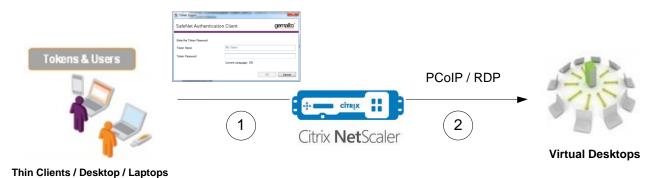
- SafeNet Authentication Client (SAC)—Version 10.0
- Citrix NetScaler Access Gateway—Version 11.0
- Citrix XenApp—Version 7.7

### Audience

This document is targeted to system administrators who are familiar with Citrix NetScaler Access Gateway, and are interested in adding certificate-based authentication capabilities using SafeNet tokens.

## **CBA Flow using SafeNet Authentication Client**

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



- A user attempts to connect to the Citrix NetScaler Access Gateway server using the Citrix NetScaler Access Gateway client application. The user inserts the SafeNet token on which his certificate resides, and, when prompted, enters the token password.
- 2. After successful authentication, the user is allowed access to select a virtual desktop machine.

SafeNet Authentication Client: Integration Guide Using SafeNet Authentication Client CBA for Citrix NetScaler Access Gateway Document PN: 007-013480-001, Rev. A, © Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries.

### **Prerequisites**

This section describes the prerequisites that must be installed and configured before implementing certificatebased authentication for Citrix NetScaler Access Gateway using SafeNet tokens:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. In general, any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, Token Policy Object (TPO) should 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 SafeNet token with an appropriate certificate enrolled on it.
- SafeNet Authentication Client (version 10.0) should be installed on all client machines.

### **Supported Tokens in SafeNet Authentication Client**

SafeNet Authentication Client (SAC) supports a number of tokens that can be used as a second authentication factor for users who authenticate to Citrix NetScaler Access Gateway.

SafeNet Authentication Client 10.0 (GA) supports the following tokens:

#### Certificate-based USB tokens

- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID and VSR

#### **Smart Cards**

- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 840
- Gemalto IDPrime MD 3810
- Gemalto IDPrime MD 3840

#### Certificate-based Hybrid USB Tokens

- SafeNet eToken 7300
- SafeNet eToken 7300-HID

#### **Software Tokens**

- SafeNet eToken Virtual
- SafeNet eToken Rescue

### **Configuring Citrix NetScaler Access Gateway**

- 1. Log in to the Citrix NetScaler administrator console.
- 2. On the **Configuration** tab, in the left pane, click **NetScaler Gateway > Policies > Authentication > CERT**.

	BYOL							Not Configured	NS11.0 64.34.nc	Logout	CITRIX.
Dashboard Configuration	Reportin	9						i	Documentation	Downloads	۰
+ System	NetScaler	> NetScaler Ga	teway > Polic	ies > Authenticatio	n > CERT > Policies					0	0 6
+ AppExpert											
+ Traffic Management	Policie	s Profiles									
+ Optimization	Add	Edit	Delete		Primary VPN Globa	al Bindings	Secondary	VPN Global Bindings			Search *
+ Security	Name	Expression			Request Server	Primary	Bound?	Primary Priority	Secondary Bound?	Seco	adary Priority
- NetScaler Gateway	No items										
<ul> <li>ture Administration</li> <li>KCD Accounts</li> <li>Policies:</li> <li>Presentation Context Switching Authorization</li> <li>Session</li> <li>ICA</li> <li>Tuffic</li> <li>TCP Compression</li> <li>Clementes Access</li> <li>Appfiow</li> <li>Authentication</li> </ul>											
- Local RADIUS											
- Web LDAP											
TACACS											
TACACS CERT SAML											

(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

- 3. In the right pane, click Add.
- 4. On the Create Authentication CERT Policy window, perform the following steps:
  - a. In the Name field, enter a name for the policy (for example, CBA\_Profile).

St NetScaler VPX AWS BYOL	HA Status Safe Not Configured NS11.0 6	64.34.nc - Logout	citrix.
Dashboard Configuration Reporting	Documen	tation Downloads	۰
+ Back			0
Create Authentication CERT Policy			
Norme* Authentication Type CR8T CR8T			
Server*			
Expression*	Expression Editor		
Operators	Clear		
Create Close			

(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

b. In the Server field, click the 📑 icon.

c. On the **Create Authentication CERT Profile** window, complete the following fields, and then click **Create**.

Name	Enter a name for the profile (for example, cert_ca).
True Factor	Select OFF.
User Name Field	Select SubjectAltName:PrincipalName.

VPN Virtual Server Authentication CERT Policy Binding 🌐 Configure Authentication CERT Policy 🗇 Create Authentication CERT Profile		
Create Authentication CERT Profile	0	×
Name" Cert_ca Authentication Type		
CRF Two Factor © ON @ OFF		
Uter Name Field SubjectAthName SPrincipalNiame Group Name Field		
Default Authentication Group		
Create Close		

(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

- d. On the Create Authentication CERT Policy window, under Expression, click Saved Policy Expressions, and then select ns\_true.
- e. Click Create.

% NetScaler VPX AWS BYOL	MA Status Mot Configured NS11.0 64.34.nc	Logout	CİTRIX'
Dashboard Configuration Reporting	Documentation	Downloads	¢
+ Back			0
Create Authentication CERT Policy			
Name" CBA.profile Authenticticion Type CBM. Server"			
cert.ca • + Cpression* Cpression* Construct • Seved Policy Expressions • Presportly Used Expressions •	Expression Editor Clear		
na_strue Croate Chose Chose			

(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

Now you need to bind the CBA authentication to the virtual server.

5. On the **Configuration** tab, in the left pane, click **NetScaler Gateway > Virtual Servers**.

	ler VPX AWS I	BYOL				Not Cont	Ngwred N512.0 64.34.oc *	Logout	citrix.
Dashboard	Configuration	Reporting					Decumentation	Downloads	۰
+ System		NetScaler 5	NetScaler Geb	nity > NetScaler Gatewa	y Virtual Servers			0	
+ AppExpert		Add		Delete Statistic	Action	-			Search *
+ Traffic Manager	ment	Name	State	IF Address	Part Protocol	Maximum Disers	Current Users	Total Com	ected Users
+ Optimization		149	. Up	183107	443 59	Addition Court //	o a	Total Color	ALCON DIST.
+ Security		celbeck	e Ve	1.0.2.103	40 55		0		
- NetScaler Gates	ay.								
Portal Theme									
Portal Theme + User Adminis KCD Account + Policies + Resources + Authentication	hyben								
+ User Adminis KCD Account + Policies + Resources + Authentication	buton b								
User Adminis KCD Account Policies     Policies     Authentication how Unlicement J	fretures								
User Administ KCD Account Policies Provides Resources Authentication Row Undicement J legrate with Clo	fretures								
+ User Adminis KCD Account + Policies + Resources	huton Is feeture Hx Products								

(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

- 6. In the right pane, select the gateway you created (for example, cag), and then click Edit.
- 7. On the VPN Virtual Server window, under Authentication, click the 📑 icon.

NetScaler VPX A	WS BYOL				@ Not	Configured NS1	1.0 64.34.nc	Logout	CİTRI
shboard Configurat	on Reporting					Docu	mentation	Downloads	•
+ Back									
PN Virtual Server									
Basic Settings						/	Help		>
Name cag IPAddress 1.0.2.102			Maximum Users Max Login Attempts	0			Advanced Sett	ings	
Port 443 State © Up RDP Server Profile -			Failed Login Timeout ICA Only Enable Authentication	false true			+ Content S	witching Policie	,
Login Once false Double Hop false			Windows EPA Plugin Upgrade Linux EPA Plugin Upgrade				+ SSL Profil	e	
Down State Flush false DTLS false AppFlow Logging false			Mac EPA Plugin Upgrade ICA Prony Session Migration Enable Device Certificate	false false			+ SSL Polici		
							+ Intranet I	P Addresses	
Certificates							+ Intranet /	Applications	
1 Server Certificate						>	+ Portal The	emes	
1 CA Certificate						>	+ EULA		
Authentication						+			
To add, please click on the +	icon						-		
SSL Parameters						/ ×			
Enable DH Param Enable DH Key Expire Size Limit Enable Ephemeral RSA Enable Session Reuse SSL Redirect	DISABLED DISABLED DISABLED DISABLED DISABLED	Clear Text Port Enable Cipher Redirect Client Authentication Client Certificate Send Close-Notify	0 DISABLED ENABLED Optional YES	SSLv2 Redirect SSLv2 SSLv3 TLSv1 TLSv1 TLSv1	DISABLED DISABLED DISABLED ENABLED ENABLED				

(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

8. On the Choose Type window, under Policies, complete the following fields, and then click Continue.

	lect CERTIFICATE.
Choose Type Sele	lect Primary.

Choose Type	×
Policies	
Choose Policy* CERTPECATE	
Choose Type*           Primary <ul> <li> </li> </ul>	
Centinue Cancel	

(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)

9. Under **Policy Binding**, in the **Select Policy** field, select the CERT policy (for example, **CBA\_Profile**) that you created earlier in step 4, and then click **Bind**.

Choose Type	
Choose Type	0 ×
Policies	1
Choose Policy CERTIFICATE	Choose Type Primary
Policy Binding	
Select Policy*       CBA_Profile     >	
▶ More	
Binding Details	
Priority* 100	
Bind Close	

(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

Now you need to configure the virtual server SSL Parameters for certificate-based authentication.

- 10. On the VPN Virtual Server window, under SSL Parameters, click the 🖄 icon, and then perform the following steps:
  - a. Clear the Enable Ephemeral RSA and Enable Session Reuse options.
  - b. Select the Client Authentication option.
  - c. In the Client Certificate field, select Optional.

SSL Parameters					×
Enable DH Param  Enable Ephemeral R  Enable Session Reus  Sable Cipher Redirect  SSLv2 Redirect  Client Authenticatio  Client Certificate*  Optional	e ect		<ul> <li>SSL Redirect</li> <li>SNI Enable</li> <li>✓ Send Close-Notify</li> <li>Clear Text Port</li> <li>0</li> <li>PUSH Encryption Trigger</li> <li>Always</li> </ul>		
Protocol					
SSLv2	SSLv3	✔ TLSv1	✓ TLSv11	✓ TLSv12	
ОК					

(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

- 11. Click OK.
- 12. Click Done.

# **Configuring Citrix StoreFront**

Configure Citrix StoreFront to allow NetScaler pass-through authentication in order to use Citrix NetScaler Gateway as the certificate-based authentication.

- 1. Open the Citrix Studio console.
- 2. In the left pane, click **Citrix StoreFront > NetScaler Gateway**.

File Action Vew Help A to be an action of the second seco
Consels Bask
Console Root
Create a new store to deliver self-service applications, data, and desktops to your users.

(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

3. In the middle pane, select the gateway you created (for example, **cag**), and then in the right pane, under **cag**, click **Change General Settings**.

Citrix Studio		EK
File Action View Help		
🗢 🔿 🔰 🖬 🖬		
<ul> <li>Console Root</li> <li>Console Root</li> <li>Citrix Studio (XenServer)</li> </ul>	alian w	Actions
Gtrix Studio (Venserver)     Gtrix StoreFront	curix	NetScaler Gateway
Server Group	Display Name Used By Services URL	Add NetScaler Gateway Appliance
Authentication Stores	cag Yes https://cag.netscaler11-demo.com	Vev
Receiver for Web		C Refresh
RetScaler Gatemay P Descors		🛿 Help
		cag
		Change General Settings
	Net Calar Catagory	Secure Ticket Authority
	NetScaler Gateway With remote access enabled, users can convect to stores from public networks through NetScaler Gateway. Users tog on once and are silently authenticated through StoreFront.	Remove NetScaler Gateway Appliance
		Help
	cag	
	URL: https://csg.netscaler11-demo.com	
	Version: 10.0 Build 69.4.0 rester	
	seatour: 10m Benno daveli ou vade.	

(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

4. On the Change General Settings window, in the Logon type field, select Smart card, and then click OK.

	640	
Display name:	cag	
NetScaler Gateway URL:	https://cag.netscaler-cba.com	
Version:	10.0 (Build 69.4) or later	*
Subnet IP address: (optional)	v10.0: SNIP or MIP, v10.1 +: VI	p
Logon type:	Smart card	*
Smart card fallback:	None	•
Callback URL: 🚺 (required)	https://cag.netscaler-cba.com	/CitrixAuthService/AuthService.asmx

(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

### **Configuring SmartCard Pass-through**

**NOTE:** It is assumed that all the appropriate configurations for smartcard single sign-on (SSO) are done. For more information, refer to http://docs.citrix.com/en-us/storefront/3/configure-authentication-and-delegation/sf-configure-smartcard.html.

1. Open the SafeNet Authentication Client Tools console.

SafeNet Authentication Client Tools						
SafeNet Authentication Client 🛛 🔅 🕸 🕯 🖗 🕸						
My Token						
AN I HAVE		Rename Token				
Gemaito Virtual Smartcard Reader 000 0	****	Change Token Password				
		Unlock Token				
	$\otimes$	Delete Token Content				
	ρ	View Token Info				
		Disconnect SafeNet eToken Virtual				
< >						
		④ GEMALTO.COM				

- 2. In the top right-corner, click the <sup>(2)</sup> icon to open the Advanced view.
- 3. In the left pane, click **SafeNet Authentication Client Tools > Tokens > Client Settings**.
- 4. In the right pane, click the **Advanced** tab, and then select **Enable single logon**.

SafeNet Authentication Client Tools		gemalto*
SafeNet Authen	tication Client	@ 😳 i ? 🚖
Safehlet Authentication Client Tools	Password Quality         Advanced           If Copy user certificates to the local store.         If Copy CA certificates to the local store.           If Copy CA certificates to the local store.         If Copy CA certificates to the local store.           If More password Quality configuration on token sher         If More password Quality configuration on token sher           If More password Quality a administrator to configure password quality configuration to token shere         Show application tray icon:           Automatic logoff after token mactivity (in minutes):         Item token mactivity (in minutes):	
( )	Enable Logging	Save Discard

5. Click Save.

I

### **Running the Solution**

### **Using SAC CBA for Citrix Web Access**

- 1. In a web browser, open the Citrix NetScaler Access Gateway URL.
- 2. On the SafeNet Authentication Client login window, enter the token password, and then click OK.

S Token Logon	reason created (descrip-		×
SafeNet Authenticat		gemalto	
Enter the Token Password			
Token Name:	My Token		
Token Password:			
	Current Language: EN		
		OK	Cancel

3. After successful authentication, you are redirected to the Citrix StoreFront console. Click on the icon of any of the published applications to launch it.

Citrix Receiver - Windows Internet Explorer		
🚱 🕗 🔹 🕲 https://csg.netscaler-cba.com/Citriu/sfWeb/		+ 🔒 🕂 🗙 🗔 ling 🖉 +
👷 Favorites 🕘 Citria Receiver		🦓 + 🔯 - 🖙 🛞 + Page + Safety + Tools + 😥 + "
Citrix StoreFront	FAVORITES APPS	
All Categories		Q, Search All Apps
All Apps		
Details Details Notepad Paint		

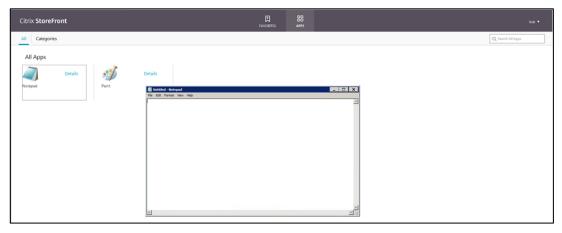
(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

4. On the **Windows Logon** window, enter your smart card PIN, and then click the Sicon.



(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

After successful authentication, you will be able to access the application.



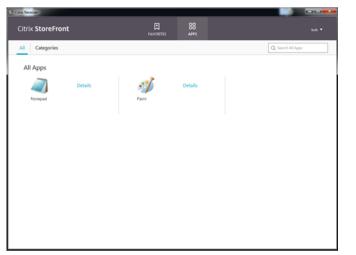
(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

### **Using SAC CBA for Citrix Receiver Application Access**

- 1. Open the Citrix Receiver application.
- 2. On the SafeNet Authentication Client login window, enter the token password, and then click OK.

Citrix StoreFront	FAVORIT	ES APPS			bob 🔻
All Categories				Q Search All Apps	
All Apps Notepad	Token Logon     SafeNet Authentication C     Erter the Token Password     Token Name: M     Token Password:	/ Taken rrent Language: EN	Gemalio C		

3. After successful authentication, you are redirected to the Citrix StoreFront console. Click on the icon of any of the published applications to launch it.



(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

4. On the **Windows Logon** window, enter your smart card PIN, and then click the Sicon.



(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

Citrix StoreFront	₽ Favoretes	BB APPS		
All Categories				Q. Search All Apps
All Apps				
Details Since Paint	Details			
Notepad Paint	Fie Edit Format View Help			
			~	
			× ×	
	1		21%	

After successful authentication, you will be able to access the application.

(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

### Using SAC CBA with SSO for Citrix Web Access

1. Log in to the client machine using the smart card for SSO.

After successful authentication, you will be logged in to the client machine.

2. Open the Citrix NetScaler Access Gateway URL in a web browser. You are redirected to access Citrix StoreFront as the SSO authentication is configured.



(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

3. Click on the icon of any of the published applications to launch it. The application will open.

Citrix StoreFront		88 895		beh 🕶
All Categories			Q Search All Apps	
All Apps Details toreput	Details			

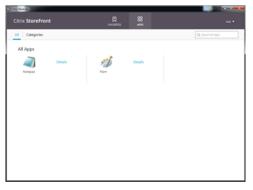
(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

### Using SAC CBA with SSO for Citrix Receiver Application Access

1. Log in to the client machine using the smart card for SSO.

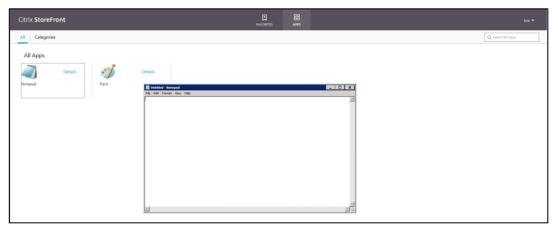
After successful authentication, you will be logged in to the client machine.

2. Open the Citrix Receiver application. You are redirected to access the Citrix StoreFront console as the SSO authentication is configured.



(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

3. Click on the icon of any of the published applications to launch it. The application will open.



(The screen image above is from Citrix<sup>®</sup>. Trademarks are the property of their respective owners.)

### Appendix: Modifying the CSP PIN Prompt from Citrix Default to SafeNet Authentication Client

- 1. Log in to the client machine as an administrator.
- 2. Open Registry Editor and then in the registry key, add the following key value:

HKLM\Software\[Wow6432Node\]Citrix\AuthManager: SmartCardPINEntry=CSP

le Edit View Favorites Help				
Computer	Name	Type REG SZ	Data (value not set)	
<ul> <li>HIKY_CLASSES.BOOT</li> <li>HIKY_CLASSES.BOOT</li> <li>HIKY_CLASSES.BOOT</li> <li>HIKY_LOCAL_MACHINE</li> <li>BCD0000000</li> <li>HARDWARE</li> <li>SAM</li> <li>SCURTY</li> <li>SOFTWARE</li> <li>SOFTWARE</li> <li>CESTEST</li> <li>Clients</li> <li>Intel</li> <li>Micrisoft</li> <li>Self-Vet</li> <li>Self-Vet</li> <li>Self-Vet</li> <li>Self-Vet</li> <li>Clients</li> <li>Self-Vet</li> <li>Self-Vet</li> <li>Clients</li> <li>Self-Vet</li> <li>Self-Vet</li> <li>Clients</li> <li>Self-Vet</li> <li>Self-Vet</li> <li>Clients</li> <li>Self-Vet</li> <li>Clients</li> <li>Self-Vet</li> <li>Clients</li> <li>Self-Vet</li> <li>Clients</li> <li>Clients<td>Provide the second seco</td><td>REG_SZ REG_SZ</td><td>(value not set) CSP</td><td></td></li></ul>	Provide the second seco	REG_SZ REG_SZ	(value not set) CSP	

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

# **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			
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017 USA			
Phone	United States International	1-800-545-6608 1-410-931-7520		
Technical Support Customer Portal		viceportal.safenet-inc.com Istomers with a Technical Support Customer Portal account can log in to cidents, get the latest software upgrades, and access the Gemalto Knowledge		