# SafeNet Authentication Client Integration Guide

Using SAC CBA for Citrix XenDesktop 7.6



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.

© 2015 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. 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: 007-013237-001, Rev. B Release Date: January 2016

## Contents

Third-Party Software Acknowledgement4
Description
Applicability
Environment5
Audience
CBA Flow using SAC
Prerequisites
Supported Tokens in SAC7
Certificate-based USB Tokens7
Smart Cards7
Certificate-based Hybrid USB Tokens7
Software Tokens7
Configuring Citrix XenDesktop 7.68
Configuring a Smart Card for the Citrix Receiver8
Configuring a Smart Card for the StoreFront Receiver for Web9
Configuring Citrix StoreFront 2.6 to Use Smart Card Pass-through Authentication10
Configuring SafeNet Authentication Client10
Configuring the StoreFront 2.6 Server11
Changing the CSP PIN Prompt from the Citrix Default to SafeNet Authentication Client11
Running the Solution12
CBA using Citrix Receiver for Web Access12
CBA Pass-through using Citrix Receiver for Web Access15
CBA using Citrix Receiver
CBA Pass-through using Citrix Receiver18
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 XenDesktop 7.6.

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 XenDesktop delivers Windows applications and desktops as secure mobile services. With XenDesktop, IT can mobilize the business, while reducing costs by centralizing control and security for intellectual property.

The XenDesktop installation installs the following components:

- Citrix StoreFront—Citrix StoreFront replaces the Citrix Web Interface and supplies web access to the XenDesktop machines. Additional information on using StoreFront can be found at the following link: http://blogs.citrix.com/2013/09/09/web-interface-or-storefront/
- Citrix Studio—Citrix Studio provides a management interface to Citrix XenDesktop and Citrix StoreFront.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Citrix XenDesktop 7.6 using SafeNet tokens.

It is assumed that the Citrix XenDesktop 7.6 environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

Citrix XenDesktop 7.6 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 XenDesktop 7.6

### **Environment**

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

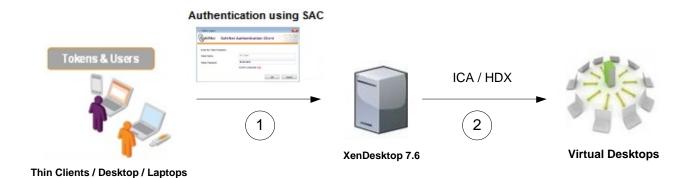
- SafeNet Authentication Client (SAC)—Version 9.0
- Citrix XenDesktop 7.6
- Citrix StoreFront 2.6

### Audience

This document is targeted to system administrators who are familiar with Citrix XenDesktop 7.6, and are interested in adding certificate-based authentication capabilities using SafeNet tokens.

### **CBA Flow using SAC**

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



- A user attempts to connect to the Citrix XenDesktop 7.6 server using the Citrix Receiver or via the StoreFront Receiver for Web. 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.

### **Prerequisites**

This section describes the prerequisites that must be installed and configured before implementing certificatebased authentication for Citrix XenDesktop 7.6 using SafeNet tokens:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. Note that any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, TPO (Token Policy Object) should be configured with a Microsoft CA connector. For additional details, refer to the "Connector for Microsoft CA" section in the SafeNet Authentication Manager Administrator's Guide.
- Users must have a SafeNet token enrolled with an appropriate certificate.
- SafeNet Authentication Client (SAC 9.0) should be installed on all client machines.

### **Supported Tokens in SAC**

SAC supports a number of tokens that can be used as second authentication factor for users who authenticate to Citrix XenDesktop 7.6.

SafeNet Authentication Client 9.0 (GA) supports the following tokens:

#### **Certificate-based USB Tokens**

- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID and VSR

#### **Smart Cards**

- SafeNet eToken PRO Smartcard 72K
- SafeNet eToken 4100

#### **Certificate-based Hybrid USB Tokens**

- SafeNet eToken 7300
- SafeNet eToken 7300-HID
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

#### **Software Tokens**

- SafeNet eToken Virtual
- SafeNet eToken Rescue

### **Configuring Citrix XenDesktop 7.6**

In this section, you will configure the various Citrix components to work with certificate-based authentication. Configure the authentication method to **Smart Card**. With this configuration method, the user will be required to enter a smart card PIN/password when logging in to the XenDesktop published machine.

#### Configuring a Smart Card for the Citrix Receiver

- 1. Open Citrix Studio.
- 2. In the left pane, select Citrix StoreFront > Authentication.

Citrix      Authentication Method     Enabled     Authentication     AddRenove Methods     Vei      AddRenove Methods     AddRenove Methods	Studio			)
Authentication Method     Enabled       Authentication Method     Enabled       Smart Card     AddRemove Methods       Smart Card     AddRemove Methods       Smart Card     Refresh       Status     Smart Card	tion View Help			
Solution     Citrixic     Authentication     Enabled     Authentication     Add/Remove Methods       Smart card     Yes     Add/Remove Methods     Yes     Add/Remove Methods       Smart card     Yes     Refeash     Refeash       Smart card     Refeash     Refeash       Smart card     Smart card     Deable Methods       Yes     Deable Method     Refeash       Smart card     To exuthentication Service     Deable Method       To exuthentication service:     https://xendesktop/Tix/authentication/auth/vi/token/validate       Number of enabled methods:     1	2 🖬 🛛 🖬			
Authentication Method     Enabled     Madifemore Methods.       Smart card     Yes     Yes       Smart card     Yes     Yes       Status     Add/femore Methods.     Yes	loot	aimur		Actions
Smart card     Yes       Series     Werr       Status     Werr	Search Machine Catalogs	cirkix		Automatica and a second s
Shart Card     rei     vel/     vel/ <td>Authentication Method</td> <td>Enabled</td> <td>Add/Remove Methods</td>		Authentication Method	Enabled	Add/Remove Methods
Image: Service and Service     Image: Service collects user credentials once and grants access to all stores on this server.       Overview     Overview       Token validation service:     https://xendesktop?l.xendes		Smart card	Yes	View +
Authentication Service     Disable Method       The authentication service collects user credentials once and grants access to all stores on this server.     Image: Control of the authentication service collects user credentials once and grants access to all stores on this server.       Overview     Toten validation service:     https://xendesktop71.xendesktopdemo.com/Cltrix/Authentication/auth/v1/token/validate       Status     Status				
Authentication Service         Deadle Method           The authentication service collects user credentials once and grants access to all stores on this server.         Image: Collects user credentials once and grants access to all stores on this server.           Overview         Toten validation service:         https://sendesktop71.xendesktopdemo.com/Clitrix/Authentication/auth/v1/token/validate           Status         Status         Image: Collect Status         Image: Collect Status				Help
Authentication Service         The authentication service collects user credentials once and grants access to all stores on this server.         Overview         Token validation service:       https://xendesktop71.xendesktopdemo.com/Citrix/Authentication/auth/v1/token/validate         Number of enabled methods:       1				Smart card
Authentication Service The authentication service collects user credentials once and grants access to all stores on this server. Overview Token validation service: https://xendesktop?l.xendesktopdemo.com/Citrix/Authentication/auth/v1/token/validate Number of enabled methods: 1 Status				Disable Method
The authentication service collects user credentials once and grants access to all stores on this server.           Overview           Token validation service:         https://xendesktop71.x	ning	Authentication Comica		🕜 Help
by Overview Token validation service: https://xendesktop71.xendesktopdemo.com/Citrix/Authentication/auth/v1/token/validate Number of enabled methods: 1 Status	Nachine Catalogo Delivery Group Polose Delivery Group Configuration Administrators Configuration Administrators Server Group StoreFront StoreFr			
Per se		The authentication service collects	user credentials once and grants access to all stores on this server.	
Token validation service: https://xendesktop71.xendesktopdemo.com/Citrix/Authentication/auth/v1/token/validate           Status	/eb	Overview		
Status				
			•	
StoreFront using HTTPS.		Status		
		StoreFront using HTTPS.		
	1.1			
	<u>) )</u>			

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

3. In the right pane, click Add/Remove Methods.

🞇 Citrix Studio				_ 8 ×
File Action View Help				
🦛 🔿 🔁 📅 🛛 🖬				
Console Root				Actions
Citrix Studio (NDSite)     Search     Machine Catalogs	CITRIX			Authentication
	Authentication Method	Enabled		Add/Remove Methods
Delivery Groups	Smart card	Add/Remove Authentication Methods		View 🕨
Cogging				Refresh
Configuration Administrators		Choose the authentication methods with which users can authenticate to stores on this server.		🕐 Help
Controllers Hosting		stores on this server.		Smart card
Licensing		User name and password		Disable Method
StoreFront StoreFront StoreFront Server Group Authentication Stores Stores Receiver for Web	Authentication Service The authentication service collects user c Overview	Domain pass-through		1 Help
RetScaler Gateway	Token validation service: https Number of enabled methods: 1	Pass-through from NetScaler Gateway OK Cancel	e	
د. (۲)	Status -			

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

4. On the Add/Remove Authentication Methods window, select Smart card, and then click OK.

#### Configuring a Smart Card for the StoreFront Receiver for Web

1. In the left pane, select **Citrix StoreFront > Receiver for Web**.

🗱 Citrix Studio				X
File Action View Help				
🗢 🔿 🖄 🖬 🔡 🖬				
Console Root				Actions
Citrix Studio (XDSite)     Search	CITRIX			Receiver for Web
Machine Catalogs	Name	Website URL	Store Authenticated	Create Website
Delivery Groups	Store Service Receiver	https://xendesktop71.xendesktopdemo.com/Citrix/StoreServiceWeb	Yes	View +
Cogging				@ Refresh
Configuration Administrators				🛃 Help
Controllers Hosting				Store Service Receiver
Licensing				Choose Authentication Methods
App-V Publishing     Citrix StoreFront	Store Service Receive	er		Add Shortcuts to Websites Change Store
Authentication				Set Session Timeout
	Overview			Deploy Citrix Receiver
	Website URL:	https://xendesktop71.xendesktopdemo.com/Citrix/StoreServiceWeb		Remove Website
P Beacons	Store: Store URL:	Store Service https://xendesktop71.xendesktopdemo.com/Citrix/Store		Help
	Store Authenticated:	Yes		
	Authentication Methods:	Smart card		
	Status			
	StoreFront using HTTP	S		
	de la companya de la			
<[				

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

2. In the right pane, click **Choose Authentication Methods**.

Root Studio (XDSite)	aimuv				Actions
studio (XDSite) earch	CITRIX				Receiver for Web
chine Catalogs	Name Websit			Store Authenticated	Create Website
elivery Groups olicies	Store Service Receiver https:/	Choose Authentication Met	hods	Yes	View
igging		<b>2 1 1 1 1</b>	n methods with which users can authenticate to the website.		G Refresh
Administrators		Choose the authenticatio	in methods with which users can authenticate to the website.		Help
Controllers Hosting		Authentication methods:	User name and password		Store Service Receiver
Licensing StoreFront		-	Domain pass-through		Choose Authentication Methods
App-V Publishing Citrix StoreFront Server Group Authentication Stores	Store Service Receiver		Smart card		Add Shortcuts to Websites
			Pass-through from NetScaler Gateway		Change Store
	Overview		- Astronogi Hommessaich Galenay		Set Session Timeout Deploy Citrix Receiver
eceiver for Web	Website URL: https:/	X A Use the Add/Remove	e Methods task to add more authentication methods.		Remove Website
NetScaler Gateway Beacons	Store: Store Store Store Store URL: https://	er			Help
	Store Authenticated: Yes Authentication Methods: Smart		OK Cancel		i ingr
	Status				
	StoreFront using HTTPS.				
	A				

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

3. On the Choose Authentication Methods window, select Smart card, and then click OK.

### Configuring Citrix StoreFront 2.6 to Use Smart Card Passthrough Authentication

Complete the procedures in this section to configure Citrix StoreFront to use smart card pass-through authentication.

### **Configuring SafeNet Authentication Client**

Enable single log on in SafeNet Authentication Client.

1. Open the SafeNet Authentication Client console.

SafeNet Authentication Client Tools	
SafeNet Authentication Client	🧶 🕼 i ? 🏦
My Token	Rename Token
	**** Change Token Password
	Unlock Token
	Delete Token Content
	View Token Info
	Disconnect SafeNet eToken Virtual
T 4 9 3 115664005 SVINCID 4 50586455 4 6 0 1 7 280 5 H R 574 F 5	www.safenet-inc.com

- 2. Click the Advanced View icon 🧼, click Client Settings, and then click the Advanced tab.
- 3. Select **Enable single logon**, and then click **Save**.

SafeNet Authentication Client Tool	5			75 <b>T</b> 68Y879U	
SafeNet				43 315 6 50\$66A 26D 5 5F4 F 5 Y	664UGS 5\16413 55 6 6 6+ Q1 5 H
SafeNet Authent	cation Client	٢	6	1	? 💼
SafeNet Authentication Client T  Solution  Solution	Password Quality Advanced Copy user certificates to the local Enable single logon Allow Password quality configur. Allow only an administrator to co Show application tray icon Automatic logoff after token inan	store ation on token after init onfigure Password quali		V V V Always Never	<b>y</b> 1 <sup>4</sup>
	🐈 Enable Logging			Save	Discard
T 4 7 3 15664UBS SV A 6 5D\$66455 6 6 9 7 260 5 H	4475 1			www.safene	t-inc.com

- 4. From the Windows **Start** menu, select **Run**, and then type **regedit.exe**, to open the Windows Registry Editor.
- 5. Complete the following steps:
  - a. Go to HKEY\_LOCAL\_MACHINE\SOFTWARE\SafeNet\Authentication\SAC, create a new key, and name it General.
  - b. In the new key, create a new DWORD (32-bit), name it **SingleLogon**, and specify a value of **1**.
  - c. Exit the Windows Registry.

#### **Configuring the StoreFront 2.6 Server**

Configure the **default.ica** file on the IIS.

- 1. Open the **default.ica** file with a text editor. (This file is typically located in C:\inetpub\wwwroot\Citrix\<Store\_Name>\App\_Data\.)
- 2. In the [Application] section, add the following setting: DisableCtrlAltDel=Off
- 3. Save the file.

For more information, go to:

http://support.citrix.com/proddocs/topic/dws-storefront-25/dws-configure-conf-smartcard.html

#### Changing the CSP PIN Prompt from the Citrix Default to SafeNet Authentication Client

Change the Citrix default CSP dialog PIN prompt to use SAC.

- 1. On the client machine where the Citrix Receiver is installed, from the Windows **Start** menu, select **Run**, and then type **regedit.exe** to open the Windows Registry Editor.
- 2. Complete the following steps:
  - a. Go to HKLM\Software\[Wow6432Node\]Citrix\AuthManager, and add the following key value: SmartCardPINEntry=CSP
  - b. Exit the Windows Registry.

For more information, go to:

http://support.citrix.com/proddocs/topic/receiver-windows-40/receiver-windows-smart-card-cfg.html

### **Running the Solution**

Check the final running solution of Citrix XenApp 7.6 and StoreFront 2.6 with SafeNet Authentication Client. In this solution, SafeNet eToken 5100 is used.

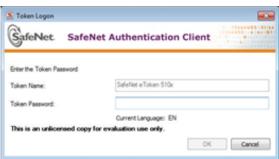
#### **CBA using Citrix Receiver for Web Access**

1. Login to the client machine using Smart card logon.



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

- 2. Open a web browser and type the StoreFront Web Receiver URL.
- 3. The **SafeNet Authentication Client** login window is displayed. Enter the **Token Password**, and then click **OK**.



After a successful authentication, you are granted access to the StoreFront Web Receiver application.



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

4. Select a machine to use. The Windows Login window is displayed.



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

5. Select the smart card authentication method, and then enter your Smart card logon PIN.

🖽 Win7 (1) - Desktop Viewer	
	bob Smart card logon bob@ssfenetdemos.com
© 🔲 🛯 🧶 W	Switch User indows 7 Enterprise

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

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

Windows 7         Windows 7         Build 7001         This copy of Windows are greatened         499 PM         7726/2015	Citr	🖽 Win7 (1) - Desktop Viewer		
Windows 7         Build 761         This copy of Windows is not sensite         Windows is not sensite         Windows 7         Build 761         This copy of Windows is not sensite	Ciu			
Windows 7         Build 701         Build 701         This copy of Windows is not genuine         Image: Second				
Windows 7         Build 701         Build 701         This copy of Windows is not genuine         Image: Second				
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015		Recycle Bin		
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015				
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015				
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015				
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015				
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015				
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015				
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015				
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015				
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015				
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015				
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015				
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015				
Build 7601           This copy of Windows is not genuine           Image: Copy of Windows is not genuine				
Build 7601           This copy of Windows is not genuine           Image: Copy of Windows is not genuine				
Build 7601           This copy of Windows is not genuine           Image: Copy of Windows is not genuine				
Build 7601           This copy of Windows is not genuine           Image: Copy of Windows is not genuine				
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015				
Build 7601           This copy of Windows is not genuine           Image: Copy of Windows is not genuine				
Build 7601           This copy of Windows is not genuine           Image: Copy of Windows is not genuine				
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015				
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015				
Build 7601 This copy of Windows is not genuine 409 PM * 7/26/2015				
This copy of Windows is not genuine				
6 10 409 PM 7/26/2015			Build 7601	
			4:09 PM	
citrix			1/26/2015	
		CITRIX		

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

#### **CBA Pass-through using Citrix Receiver for Web Access**

1. Login to the client machine using **Smart card logon**.



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

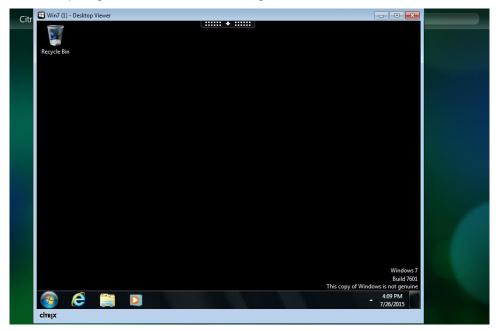
2. Open a web browser and type the Citrix Receiver for Web URL.

Since Citrix is configured for pass-through authentication, the user is not required to enter the smart card PIN code, and is automatically logged in to the Citrix StoreFront web portal.



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

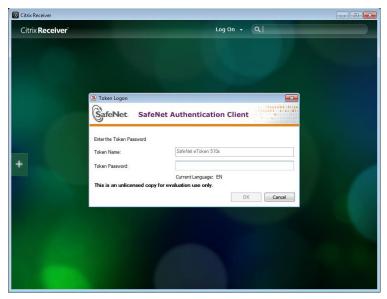
3. Select a machine to use. Since Citrix is configured for pass-through authentication, the machine will open without requiring the user to authenticate again.



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

#### **CBA using Citrix Receiver**

- 1. Insert the selected SafeNet eToken or smart card.
- 2. Launch Citrix Receiver. The **SafeNet Authentication Client** opens. Enter the **Token Password**, and then click **OK**.



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

After a successful authentication, the Citrix Receiver application window is displayed.



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

3. Select a virtual desktop. The Windows Login window is displayed.



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

4. Select the smart card authentication method, and then enter your **Smart card** PIN. After a successful authentication, you will be logged on to the virtual desktop.

Citr	🖽 Win7 (1) - Desktop Viewer		
Ciu			
	Recycle Bin		
		Windows 7	
		Build 7601	
	This copy of W	indows is not genuine	
	🚳 😂 🚞 🗵	4:09 PM 7/26/2015	
	citrix		

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

#### **CBA Pass-through using Citrix Receiver**

1. Log in to the Windows client workstation using Smart card logon.



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

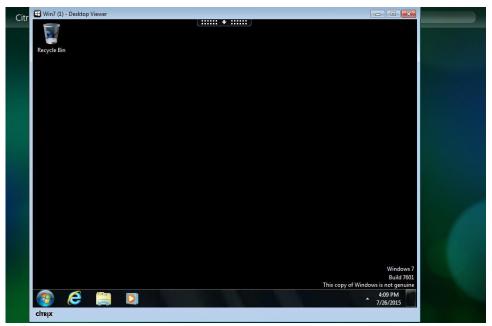
2. After successful authentication, launch Citrix Receiver.

Since Citrix is configured for pass-through authentication, you are not required to enter the smart card PIN code, and are automatically logged in to Citrix Receiver.



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

3. Select a virtual desktop. Since Citrix is configured for pass-through authentication, the virtual desktop can be accessed without requiring you to authenticate again.



(The screen image above is from Citrix<sup>®</sup>. 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, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA			
Phone	United States	1-800-545-6608		
	International	1-410-931-7520		
Technical Support Customer Portal		ting customers with a Technical Support Customer Portal account can log in to age incidents, get the latest software upgrades, and access the Gemalto Knowledge		