SafeNet Authentication Client

Integration Guide

Using SafeNet Authentication Client CBA for Citrix Linux Receiver

gemalto
security to be free

Document Number: 007-013962-001, Rev. A

Release Date: November 2017

Contents

Third-Party Software Acknowledgement

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

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, such as 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.

Receiver for Linux enables users to access virtual desktops and hosted applications delivered by XenDesktop and XenApp from devices running the Linux operating system.

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

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

Citrix Linux Receiver 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) Typical installation mode**— SafeNet Authentication Client is public key infrastructure (PKI) middleware that manages Gemalto's tokens and smart cards.

  For more details about different SAC installation modes, please refer to Customization section in *SafeNet Authentication Client Administrator Guide*.

- **Citrix Linux Receiver**

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 Linux Receiver** - *version 13.7*
- **Citrix XenApp/XenDesktop** - version 7.14
- **Linux RedHat** - version 7.3

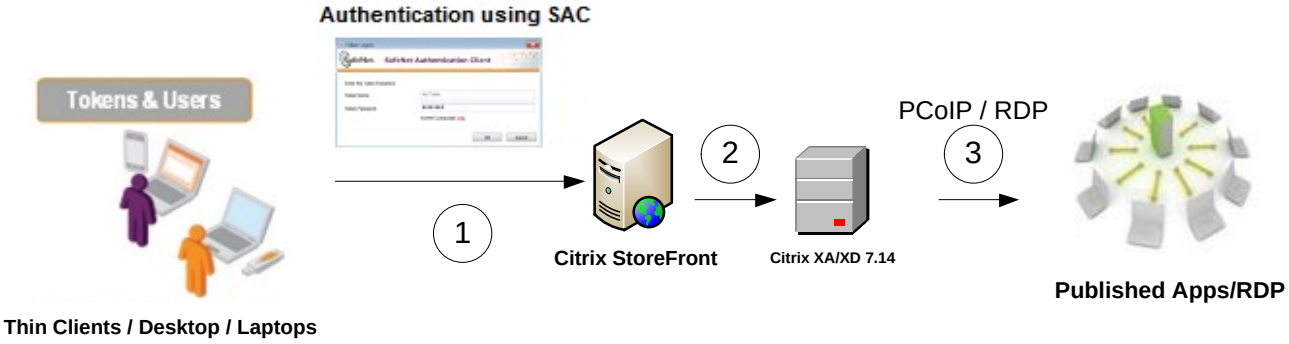
Audience

This document is targeted to system administrators who are familiar with Citrix Linux Receiver, and are interested in adding certificate-based authentication capabilities using Gemalto tokens and smart cards.

See "Supported Tokens and Smart Cards in SafeNet Authentication Client," on page 7.

CBA Flow using SafeNet Authentication Client

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



1. A user attempts to connect to the Citrix Linux Receiver server using the Citrix Receiver for Linux. The user inserts the Gemalto SafeNet token or Smartcard on which his certificate resides, and when prompted, enters the token password.
2. After successful authentication, the user is allowed access to the published apps/desktops.
3. The user selects the app/desktop to use.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based authentication for Citrix Linux Receiver 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 SafeNet Authentication Manager (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 for Linux 10 must be installed on all Linux client machines.

Supported Tokens and Smart Cards in SafeNet Authentication Client

SafeNet Authentication Client for Linux 10.0 supports the following tokens and smart cards:

Certificate-based USB tokens

- SafeNet eToken 5110 GA
- SafeNet eToken 5110 FIPS

Smart Cards

- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 840

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

Configuring Citrix Linux Receiver

This section demonstrates how to configure Citrix Linux receiver to support Gemalto tokens and smart cards. In our lab we used a Microsoft local CA, so first we will configure the Citrix Linux Receiver to trust the local root CA certificate.

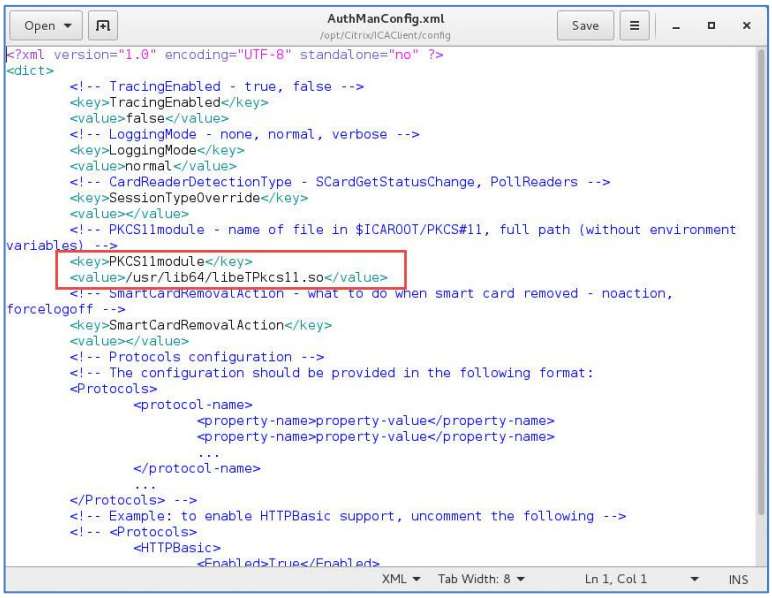
1. Login to the local certificate authority and download the Root CA certificate. Make sure you download the certificate in **Base64 Encoding**.
2. Rename the certificate file to **pem**
3. Copy the certificate to **/opt/Citrix/ICAClient/keystore/cacerts/**
4. Run the following command: **/opt/Citrix/ICAClient/util/ctx_rehash**

   Now the Citrix Receiver is able to trust the local CA.

Next, we will add SafeNet Authentication Client PKCS#11 support to the Citrix Linux Receiver:

1. Open the file **/opt/Citrix/ICAClient/config/AuthManConfig.xml** in an editor.
2. Under the key PKCS11module key enter the following value (path to SafeNet Authentication Client PKCS#11 dll):

   <value>/usr/lib64/libeTPkcs11.so</value>

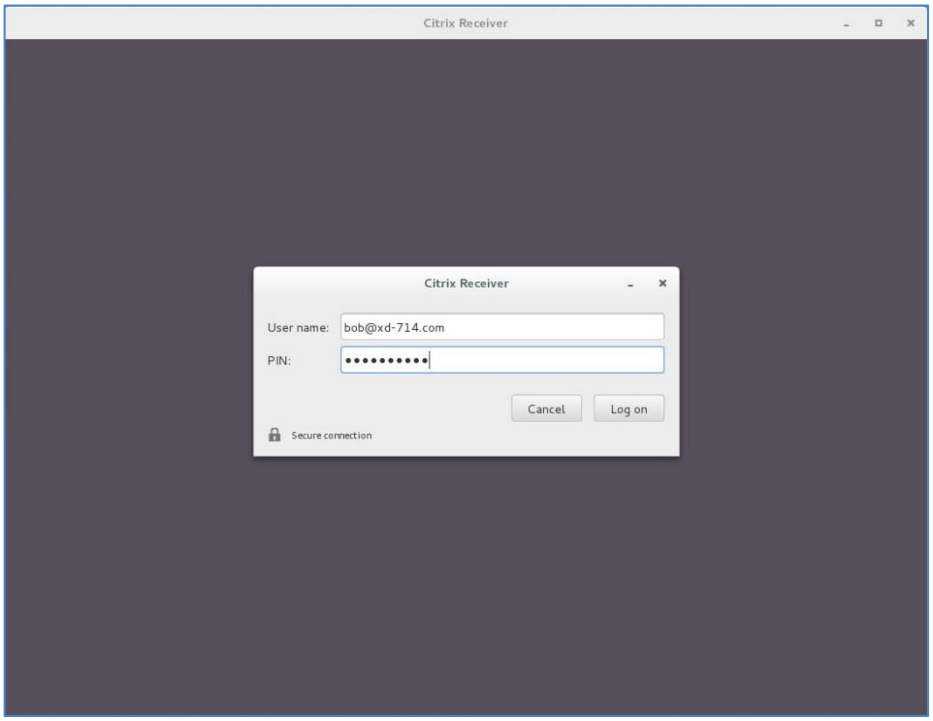


3. Save the file and restart the machine.

Running the Solution

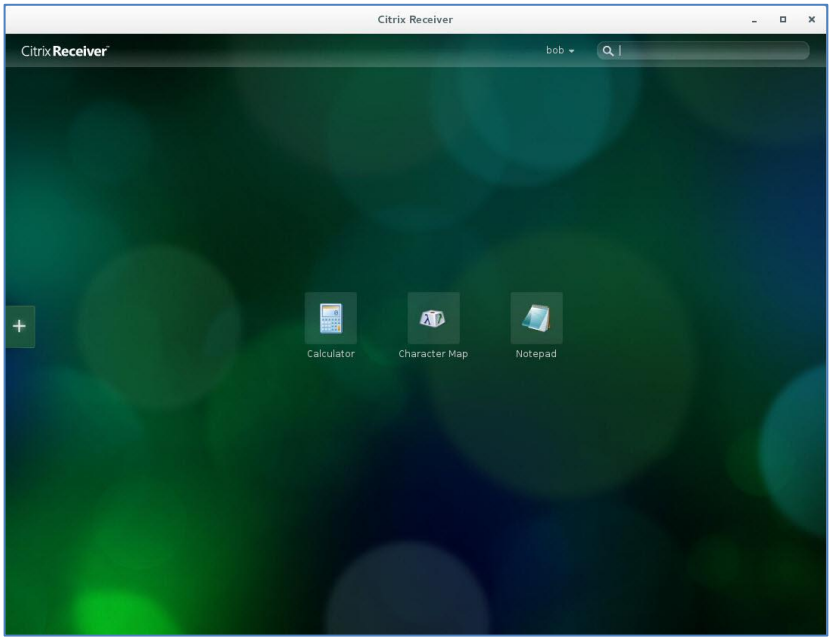
In this lab we used Citrix XenApp/XenDesktop 7.14 with Linux Receiver 13.7 installed on RHEL 7.3.

1. The Linux user inserts a Gemalto token or smart card.
2. The user opens the Citrix Receiver and is prompted to enter the token/smart card PIN code.



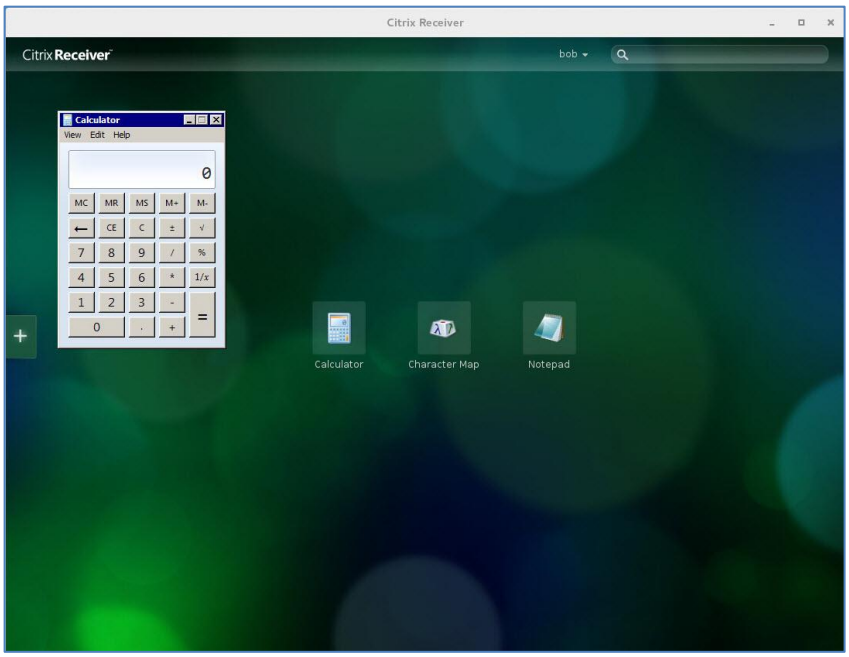
(The screen image above is from Citrix Systems, Inc. Trademarks are the property of their respective owners).

3. After clicking **Log on** the user is authenticated to the Citrix StoreFront.



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

4. Now, the user can run an app and it will be executed without being required to re-authenticate.



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

Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support.

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

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

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

Telephone Support

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

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

Region	Telephone number (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Korea	+82 2 3429 1055
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