

SafeSign Identity Client User Guide

Citrix Presentation Server 4.5

This document contains information of a proprietary nature.

No part of this document may be reproduced or transmitted in any form or by any means electronic, mechanical or otherwise, including photocopying and recording for any purpose without written permission of A.E.T. Europe B.V.

Individuals or organisations, which are authorised by A.E.T. Europe B.V. in writing to receive this information, may utilise it for the sole purpose of evaluation and guidance.

A.E.T. Europe B.V.
IJsselburcht 3
NL - 6825 BS Arnhem
The Netherlands

Warning Notice

All information herein is either public information or is the property of and owned solely by A.E.T. Europe B.V. 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.

This information is subject to change as A.E.T. Europe B.V. reserves the right, without notice, to make changes to its products, as progress in engineering or manufacturing methods or circumstances warrant.

Installation and use of A.E.T. Europe B.V. products are subject to your acceptance of the terms and conditions set out in the license Agreement which accompanies each product. 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 A.E.T. Europe B.V. information.

Cryptographic products are subject to export and import restrictions. You are required to obtain the appropriate government licenses prior to shipping this Product.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, A.E.T. Europe B.V. 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, A.E.T. Europe B.V. reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

A.E.T. EUROPE B.V. 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 A.E.T. EUROPE B.V. 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.

© Copyright A.E.T. Europe B.V., 1997-2007.

All rights reserved.

SafeSign Identity Client is a trademark of A.E.T. Europe B.V. All A.E.T. Europe B.V. product names are trademarks of A.E.T. Europe B.V. All other product and company names are trademarks or registered trademarks of their respective owners.

Credit information:

This product includes cryptographic software written by Eric A. Young (ey@cryptsoft.com)

This product includes software written by Tim J. Hudson (tjh@cryptsoft.com).

Contact Information: A.E.T. Europe B.V.

IJsselburcht 3
NL-6825 BS
P.O. Box 5486
NL-6802 EL Arnhem
The Netherlands
Tel. +31-26-365 33 50
Tel. Support +31-26-365 35 43
Fax +31-26-365 33 51



info@aeteurope.nl / support@aeteurope.nl
<http://www.aeteurope.com/>

SafeSign Identity Client is a product developed by
A.E.T. Europe B.V.

Copyright © 1997 - 2007 A.E.T. Europe B.V.,
Arnhem, The Netherlands.
All rights reserved.



Document Information

Filename: SafeSign Identity Client User Guide
Citrix Presentation Server 4.5

Document ID: Citrix_Presentation_Server_4.5_SafeSign_v2.3.2_User_Guide

Project Information: SafeSign Identity Client Documentation

Document revision history

Version	Date	Author	Changes
1.0	16-05-2007	Mustafa Abarkan	First edition for SafeSign Identity Client Standard Version 2.3 (release 2.3.2)

WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE

Table of contents

Warning Notice	I
Document Information	II
Table of contents	III
Table of figures	IV
Introduction	V
About the Product	VI
About the Manual	VII
1 Citrix Presentation Server 4.5	1
1.1 SafeSign Identity Client for Citrix.....	1
1.2 Prerequisites.....	1
2 Authentication with Citrix	2
2.1 Installation of ICA.....	2
3 Smartcard Logon with Citrix and SafeSign Identity Client	8
3.1 ICA configuration settings.....	8
3.2 Smartcard logon configuration settings.....	12

Table of figures

Figure 1: Installation file Citrix	2
Figure 2: Begin Installation Citrix	2
Figure 3: Server Client Setup	3
Figure 4: Choosing Server URL	3
Figure 5: Selecting Program Folder	4
Figure 6: Selecting Machine Name	4
Figure 7: Local Name and Password.....	5
Figure 8: Additional Settings.....	5
Figure 9: Installation Summary.....	6
Figure 10: Updating features	6
Figure 11: Successful Installation.....	7
Figure 12: Desktop Icon	8
Figure 13: Application Set Manager	8
Figure 14: Custom ICA Connections	9
Figure 15: Add ICA Connection	9
Figure 16: Type of Connection	9
Figure 17: Connection Description.....	10
Figure 18: Server Location and Name.....	10
Figure 19: Encryption Level	10
Figure 20: User name, Password & Domain	11
Figure 21: Window Colors and Size	11
Figure 22: Application and Working Directory	11
Figure 23: Finish Setup	12
Figure 24: SafeSign Citrix Connection.....	12
Figure 25: Connection Properties	13
Figure 26: Logon Information	13
Figure 27: Option Smart Card	14
Figure 28: Desktop Icon	14
Figure 29: Preparing to Connect	14
Figure 30: Connection Established.....	15
Figure 31: Checking Credentials.....	15
Figure 32: Card Insertion.....	15
Figure 33: PIN Request	15
Figure 34: Entering PIN.....	16
Figure 35: Starting Citrix Desktop	16
Figure 36: Working Desktop Connection	16

Introduction

This document describes how to implement smartcard logon using Citrix and SafeSign Identity Client. It will guide you through the process of installation and configuration needed for a connection with Citrix. Also, you will find the prerequisites described in this document.

The first chapter gives you a brief description of the functionalities of Citrix and treats the installation of the necessary components needed for optimal performance of the connection.

The second chapter gives a detailed instruction how to install the ICA client.

The third chapter is dedicated to the configuration of Citrix to enable smartcard logon.

After reading this document you will be able to make a connection with Citrix (desktop) using smartcard logon.

About the Product

SafeSign Identity Client is a software package that can be used to enhance the security of applications that support hardware tokens through PKCS #11 and Microsoft CryptoAPI.

The SafeSign Identity Client package provides a standards-based PKCS #11 Library and Cryptographic Service Provider (CSP), allowing users to store public and private data on a personal token, either a smart card, USB token or SIM card. It also includes the SafeSign Identity Client PKI applet, enabling end-users to utilise any Java Card 2.1.1 and higher compliant card with the SafeSign Identity Client middleware.

Combining full compliance with leading industry standards and protocols, with flexibility and usability, SafeSign Identity Client can be used with multiple smart cards / USB tokens, multiple Operating Systems and multiple smart card readers.

SafeSign Identity Client allows users to initialise and use the token for encryption, authentication or digital signatures and includes all functionality necessary to use hardware tokens in a variety of PKI environments.

SafeSign Identity Client Version 2.3 for Windows supports the following tokens (as described in the product description):

- STARCOS® smart cards developed by Giesecke & Devrient GmbH (G&D): SPK2.3, SPK2.3 RawRSA, SPK2.4, SPK2.4 FIPS, SPK2.5 Dual Interface (DI) and STARCOS 3.0;
- The G&D StarKey100 (M) and StarKey200 USB token with the completed STARCOS SPK 2.3 / 2.4 operating system;
- The G&D StarKey220 HID token with the completed STARCOS SPK 2.3 operating system;
- The G&D StarKey400 and StarKey400 M (with flash memory) USB token with Sm@rtCafé Expert 64k;
- The Eutron Cryptoidentity / CryptoCombo ITSEC-P with the completed STARCOS SPK 2.3 operating system, and the Cryptoidentity / CryptoCombo FIPS USB token with the completed STARCOS SPK 2.4 operating system;
- The KeyCorp Multos v4.2 48K card and the KeyCorp Multos v4.2 64K card;
- Java Card v2.1.1 / Open Platform 2.0.1 compliant Java smart cards:
Aspects OS755 v2.8, Axalto e-gate, Axalto Cyberflex Access Developer 32K, Axalto Cyberflex 64Kv1 and 64Kv2, Axalto Cyberflex Palmera, G&D Sm@rtCafé Expert 2.0, G&D STARSIM Java, Gemplus GemXpresso 211pk/Pro R3, IBM JCOP 20/21/30/31, MartSoft Java card, Oberthur CosmopolIC v4 and Orga JCOP 20/30.
- Java Card v2.2+ / GlobalPlatform 2.1.1 compliant Java smart cards:
Aspects OS755 (Java Card 2.2), G&D Sm@rtCafé Expert 64, G&D Sm@rtCafé Expert 3.0, G&D Sm@rtCafé Expert 3.1, IBM JCOP21 (Java Card 2.2), IBM JCOP31 (Java Card 2.2), IBM JCOP41, Oberthur IDOne Cosmo64 v5.2, Oberthur IDOne Cosmo 64 RSA D/T v5.4 and Oberthur IDOne Cosmo 32 RSA v3.6.

SafeSign Identity Client comes in a standard version with an installer for the following Windows environments¹:

- Windows 2000, Windows XP (Professional), Windows 2003 Server, Windows Vista.

In principle, SafeSign Identity Client supports any PC/SC compliant smart card reader. However, to avoid power problems, smart card readers must be capable to provide at least a current of 60mA. PC/SC driver software is available from the web site of the smart card reader manufacturer.

For more information, refer to the latest SafeSign Identity Client Product Description.

¹ Windows NT 4.0 is supported up to SafeSign Identity Client 1.0.9.04, in line with Microsoft's end-of-life policy. Windows 98 and Windows ME are supported up to SafeSign Identity Client 2.3.0 (< 2.3.0), in line with Microsoft's end-of-life policy.

About the Manual

This manual is specifically designed for users of Citrix Presentation Server 4.5, who wish to use their SafeSign Identity Client Token to enhance the security of their communications.

The manual describes how to work with your SafeSign Identity Client Token in combination with Citrix Presentation Server 4.5.

In order to set up your SafeSign Identity Client Token for use with Citrix Presentation Server, follow the instructions in the manual.

Note that this manual assumes you have installed SafeSign Identity Client and have initialised the token with the SafeSign Identity Client Token Management Utility / Token Administration Utility, thus making it ready to use with Internet Explorer and Microsoft applications. See for instructions on installing SafeSign Identity Client the *SafeSign Identity Client User Guide for Installation* and for configuring and managing your SafeSign Identity Client Token, either the *SafeSign Identity Client Token Management Utility Guide* or *SafeSign Identity Client Token Administration Utility Guide*.

This manual also assumes that you have installed Citrix Presentation Server 4.5. In order to install Citrix Presentation Server 4.5 we refer to the documentation of Citrix. This documentation is available on the website of Citrix².

This document is part of the user documentation for SafeSign Identity Client.

² <http://www.citrix.com>

1 Citrix Presentation Server 4.5

Citrix Presentation Server is a remote end-to-end access/application publishing program that gives users remote access to a server desktop or (an) application(s) through "thin client" software. It is also possible to use it on regular desktops. One advantage is that it enables access for a remote user with several devices, on different networks. It allows companies to provide secure - by allowing the user to authenticate to Citrix, with key(s) and certificates stored on a token - applications on different IT platforms and operating systems.

With Citrix Presentation Server, you can access published applications or the desktop itself on virtually any computing device. When a user runs an application on Citrix, all of the application execution takes place on the server, and only keyboard, mouse, and display information traverses the network. Users see only their own individual sessions, which are managed transparently by the server operating system, and remain independent of any other client session. Through terminal emulation, Citrix allows the same set of applications to run on diverse types of desktop hardware.

This document describes the possibilities to implement smartcard logon using SafeSign Identity Client and Citrix.

1.1 SafeSign Identity Client for Citrix

SafeSign Identity Client for Citrix ICA Client is a double authentication method to give users a safe and secure smart card (or USB token) authentication to Citrix Presentation Servers. It gives the opportunity to Citrix users to utilize their accounts without having to memorize their passwords. This puts an end to losing the password and is very convenient for an efficient password management.

Logon with SafeSign Identity Client for Citrix users provides the ability to securely store user data and certificates on a smart card (or USB token) and use them whenever necessary.

It is possible to log in with SafeSign Identity Client without changing any features or installing additional components. If you want to know more about the different features of Citrix, we refer to the documentation available from Citrix.

1.2 Prerequisites

For smart card logon with Citrix Presentation Server in Windows 2003 Server to work, the following prerequisites are to be fulfilled:

- Smartcard logon configured on the domain;
- A Certification Authority installed and configured;
- SafeSign Identity Client software installed on the Windows 2003 (Terminal) Server enabling Smart Card Logon;
- Drivers for the smart card reader(s) installed on the client;
- A smart card reader installed on the client;
- A token (smart card or USB token) that is supported by SafeSign Identity Client, personalized with a Digital ID which supports smart card logon (see the *SafeSign Identity Client User Guide for Microsoft Windows 2003* for more details) for use on the client;
- Windows 2000, Windows XP, Windows Server 2003 or a "thin client" used as a client to connect to the Citrix Server;
- Citrix Presentation Server 4.5 installed on the Server;
- Citrix ICA Client installed on the client and configured (see installation guide) (i.e. a version which supports Smartcard Logon).

In order to have a functioning environment it is recommended to have two servers. One server with the Certification Authority, the other server with Citrix installed. On the client only the ICA Client has to be installed. SafeSign Identity Client has to be installed on all servers involved.

2 Authentication with Citrix

In order to be able to use Citrix on a client, you need to install the ICA-client. ICA means 'Independent Computing Architecture'. The idea of ICA is that a desktop only needs components to receive and show remote desktop images and to send the responses of the user to a central Citrix-server. Communication takes place using the ICA-protocol. The Citrix server takes care of all other processes (application processes, communication with the database etc.).

2.1 Installation of ICA

To install ICA, you need to have the CD with Presentation Server Components:

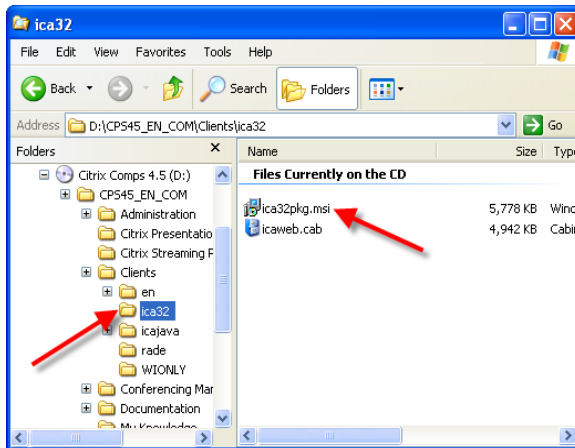


Figure 1. Installation file Citrix

1. Select the folder *:\CPS45_EN_COM\Clients\ica32
2. Double click on the *.msi file ica32pkg.msi

The following screen appears:



Figure 2: Begin Installation Citrix

Wait a few seconds until the next screen appears:

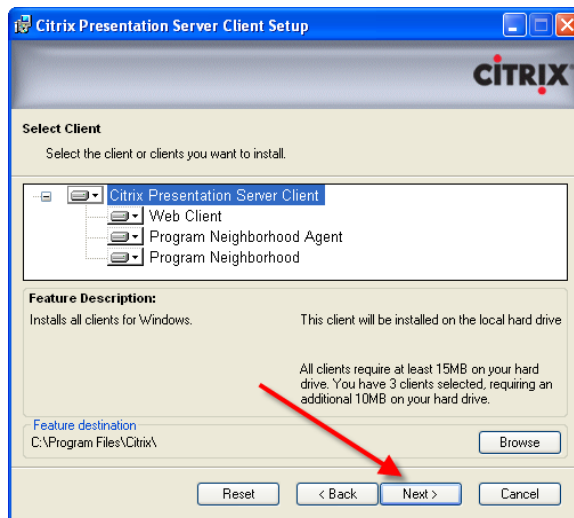


Figure 3: Server Client Setup

Here you can install all the necessary clients on your computer. Select all clients and click on "Next".

Then the following screen appears:

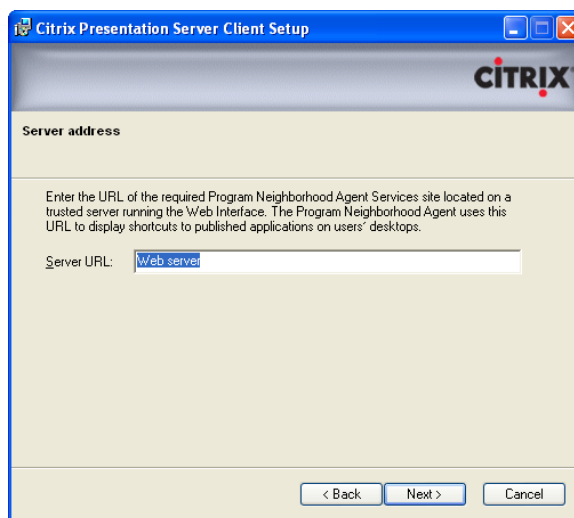


Figure 4: Choosing Server URL

Depending on which configuration Citrix is running, you need to enter the URL of the required Program Neighborhood Agent Services. This is only needed when you are running a web client.

Click on "Next" to continue the configuration.

If you want the icon of Citrix to be placed in another file, you can change this by entering the preferred location:

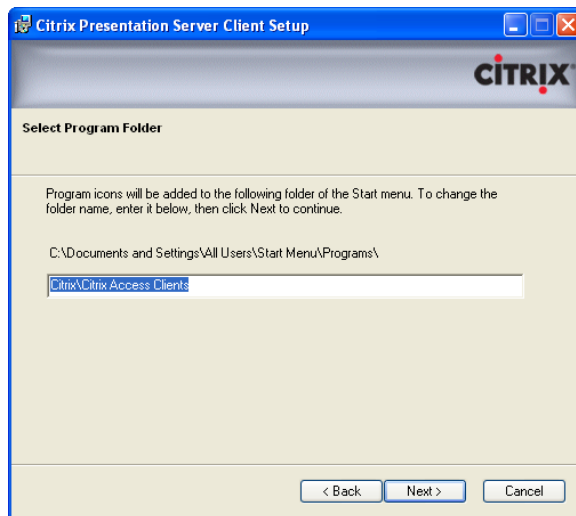


Figure 5: Selecting Program Folder

Click on "Next" and proceed with the configuration.

Then the following screen appears:

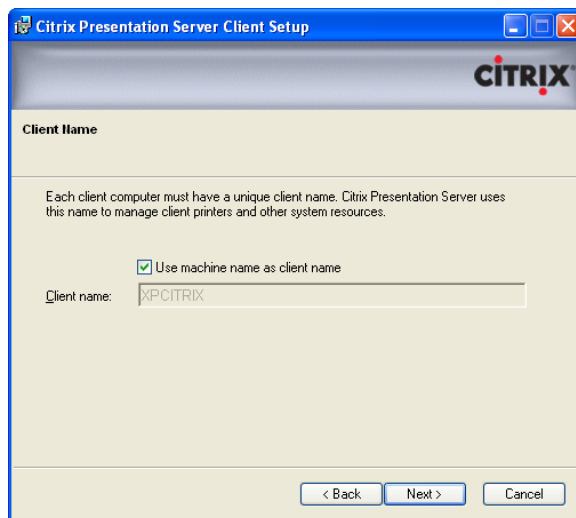


Figure 6: Selecting Machine Name

In this setup screen you can change the client name. Use the name of your client and click on "Next".

For smartcard logon you don't need to use your local user name and password:

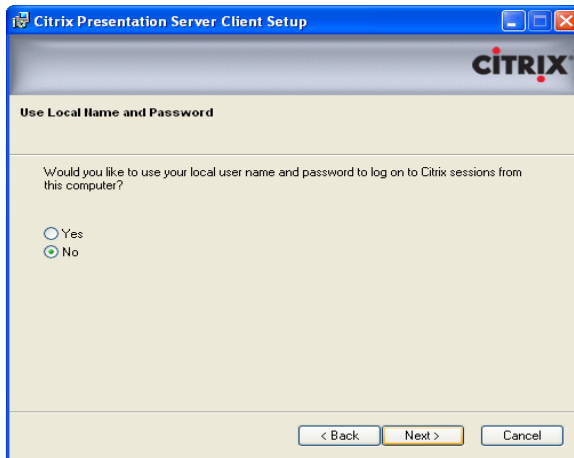


Figure 7: Local Name and Password

Select "No" and click on "Next".

Select the two options "Enable Quick Launch Bar" and "Enable Custom ICA Connections" and click on "Next":

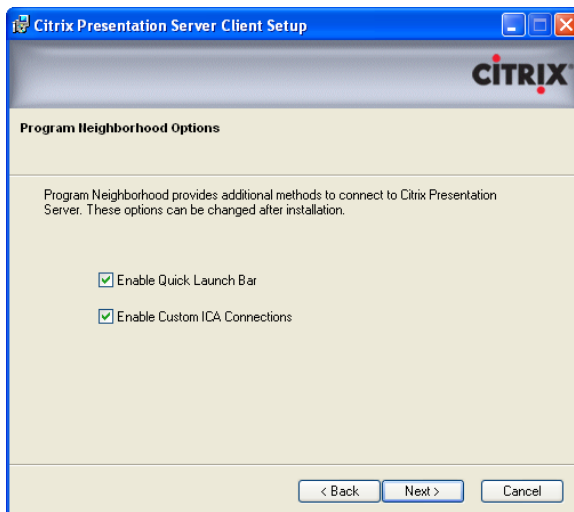


Figure 8: Additional Settings

The setup screen below shows the selected Citrix components to be installed:

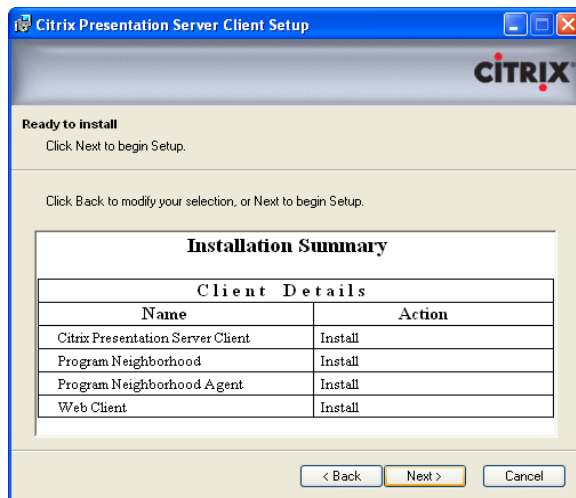


Figure 9: Installation Summary

You now can click on "Next".

The following screen will appear and Citrix will install all of the selected features:

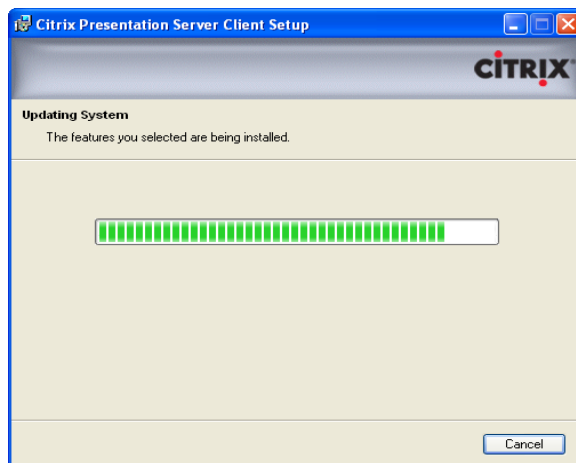


Figure 10: Updating features

Citrix installs the selected components and updates the system if needed. Wait until the next screen appears.

After this installation procedure you will have installed Citrix ICA successfully and the following screen will show:



Figure 11: Successful Installation

You have successfully installed Citrix Presentation Server Client and you are ready to use Citrix from your desktop.

3 Smartcard Logon with Citrix and SafeSign Identity Client

3.1 ICA configuration settings

After having successfully installed the ICA-client on your computer, an icon of Citrix can be found on your desktop:



Figure 12: Desktop Icon

Double click on the "Citrix Program Neighborhood" icon.

Double click on "Application Set Manager":

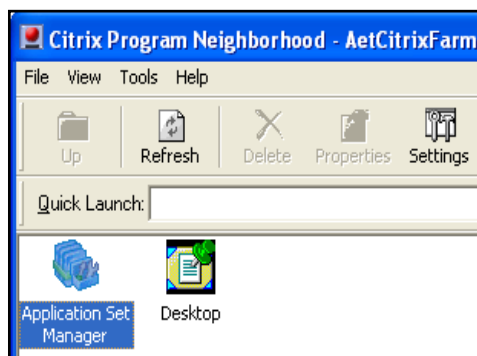


Figure 13: Application Set Manager

In the next screen you will find an icon named “Custom ICA connections”. This feature enables the user to login with Citrix:

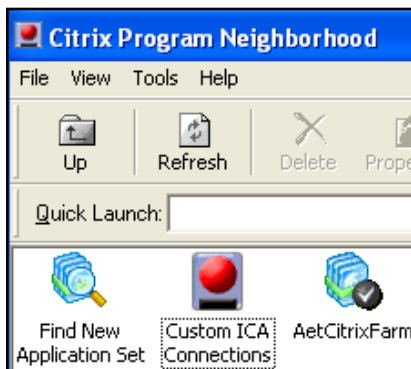


Figure 14: Custom ICA Connections

Double click on the icon “Custom ICA Connections”.

You now can add an ICA connection which enables you to make contact with the Citrix server. Double click on the icon “Add ICA Connection”:

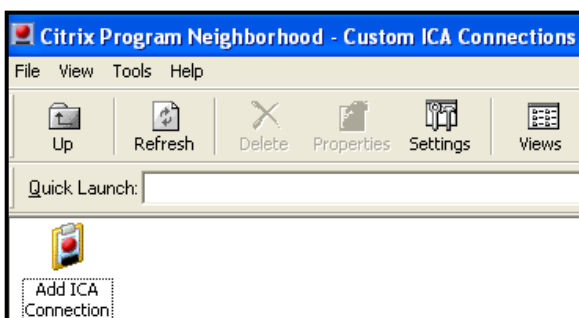


Figure 15: Add ICA Connection

After double clicking the icon, the screen below will show. Here you can select the type of connection you will use for the new application:

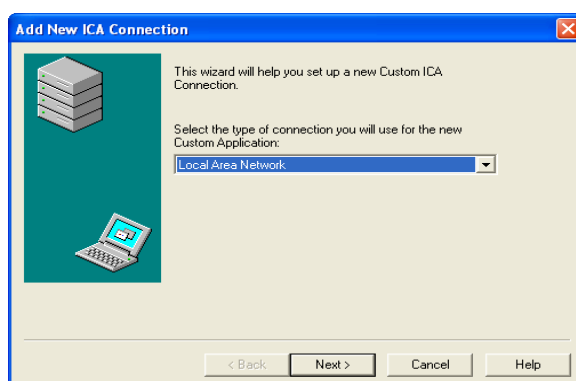


Figure 16: Type of Connection

Select the type of connection and click on “Next”.

Enter a description for the new ICA connection. In this example we named the connection “SafeSign Citrix Connection”:

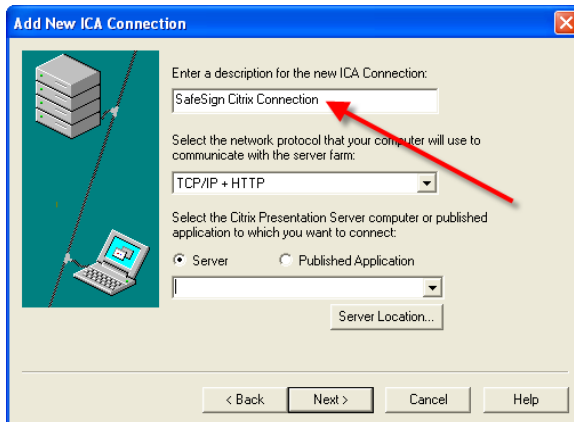


Figure 17: Connection Description

Select the network protocol that your computer will use to communicate with the server farm. Then select/enter the name of the server to which you want to make a connection:

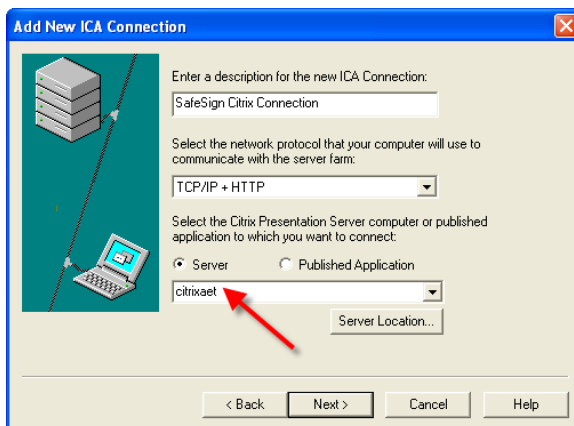


Figure 18: Server Location and Name

In this case we selected the name of the server “citrixact”. After completing filling in the necessary information, click on “Next”.

Use the default settings of the ICA connection and enable session reliability. After finishing those settings, you can click on “Next”:

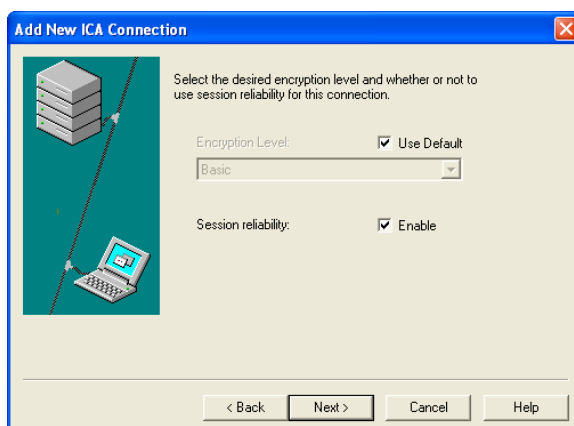


Figure 19: Encryption Level

To make the configuration of smartcard logon easier, it is preferable not to fill in a User name, password and domain. Leave these fields blank so you will be prompted for this information when you connect and click on "Next":

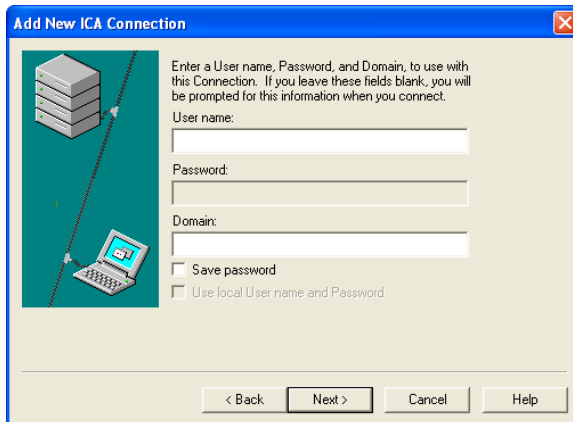


Figure 20: User name, Password & Domain

In this window you can determine which Window Colors and Window Size will be used by Citrix. Select the preferred option and click on "Next":

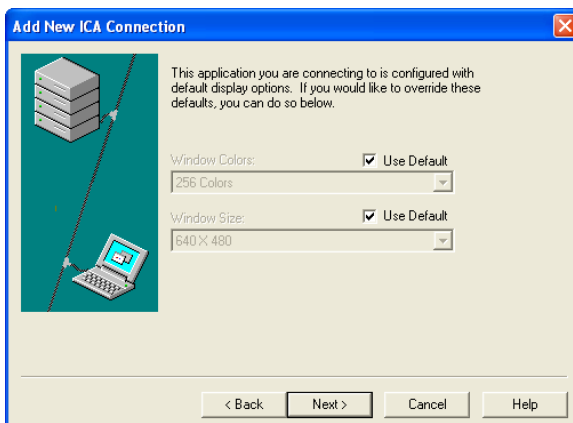


Figure 21: Window Colors and Size

The window here below can be used to enter a filename or application which is to be used at start up. In this example the box will be left empty:

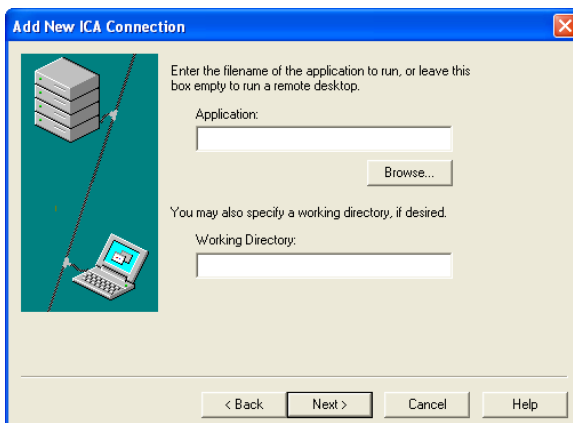


Figure 22: Application and Working Directory

After choosing the filename/application, you can click on "Next".

You have successfully configured the ICA connection. Click on “Finish” to close the set up.

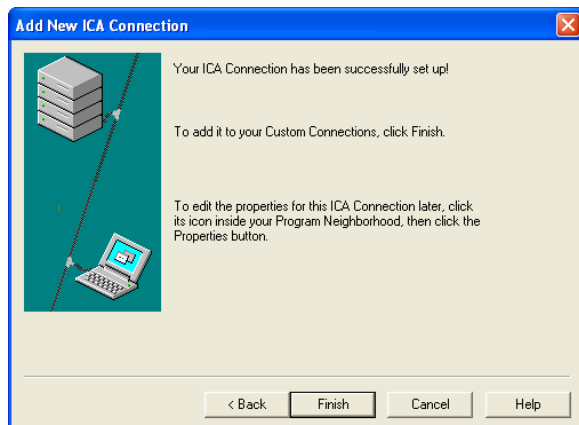


Figure 23: Finish Setup

Now we will set up smartcard logon authentication with Citrix.

3.2 Smartcard logon configuration settings

After finishing the configuration of the ICA connection, you need to set up the smartcard logon options. First you will see a new icon with the chosen name (SafeSign Citrix Connection) as displayed in the next figure:

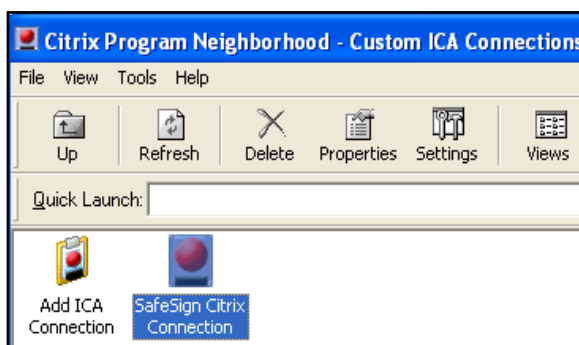


Figure 24: SafeSign Citrix Connection

Right click on the icon (SafeSign Citrix Connection) and click on the option "Properties":

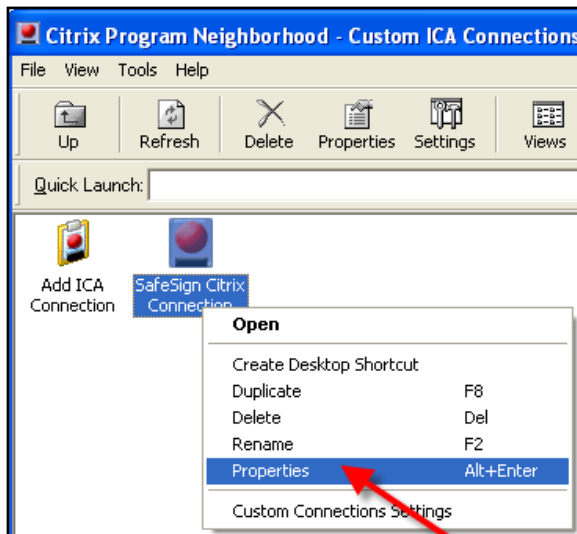


Figure 25: Connection Properties

After selecting "Properties", you will be able to configure the logon settings. This is displayed in the figure below:

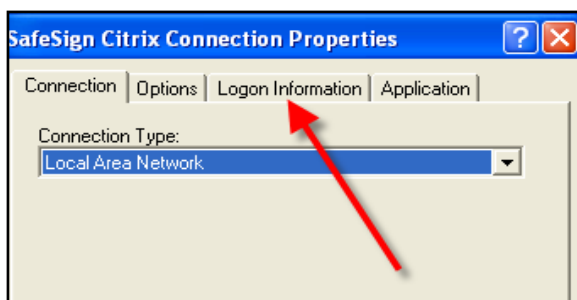


Figure 26: Logon Information

After clicking on "Logon Information" you can configure the method how to log on with Citrix.

Continue the configuration by selecting "Smart Card".

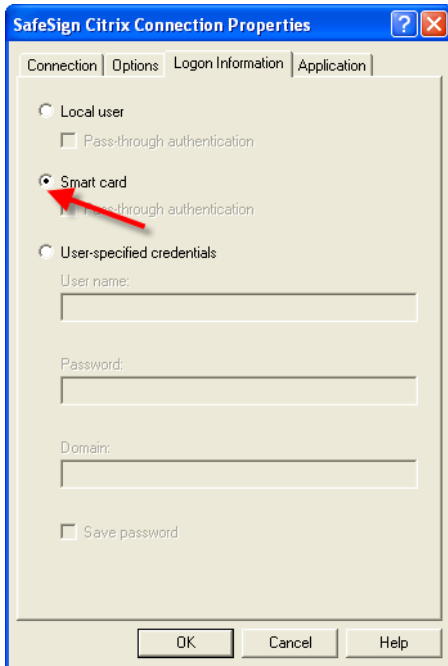


Figure 27: Option Smart Card

Leave all other options unselected and click on "OK". Copy the icon "SafeSign Citrix Connection" to your desktop in order to make logon easier to find:



Figure 28: Desktop Icon

After placing an icon on the desktop, you will be able to log on with a smartcard by double-clicking on it. The next screen will appear:



Figure 29: Preparing to Connect

Wait a few seconds in order to let the Citrix server connect to your desktop. After that, the next message will show on the Citrix window: "Connection established. Negotiating capabilities...":



Figure 30: Connection Established

Citrix will start checking your credentials on the smartcard. Wait until this process finishes:



Figure 31: Checking Credentials

After checking your credentials, the login screen will appear:



Figure 32: Card Insertion

Insert your token and wait for instructions.

The Windows Server will ask for your PIN:

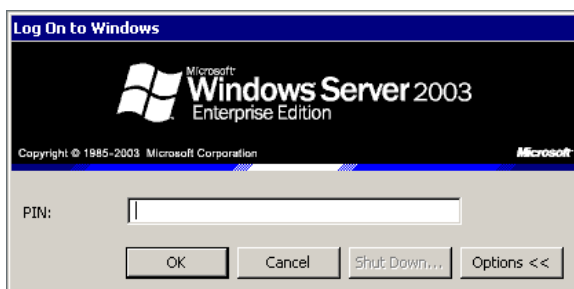


Figure 33: PIN Request

You can enter your PIN and click on “OK”:

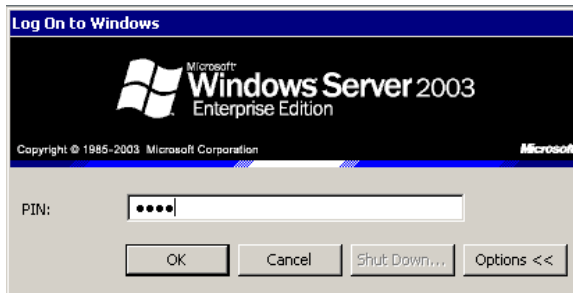


Figure 34: Entering PIN

Citrix will establish a connection. In this example the configuration is set to make a connection with the desktop:



Figure 35: Starting Citrix Desktop

After examining and applying your personal settings, the desktop of the remote server will appear. You are now ready to use the Citrix connection:

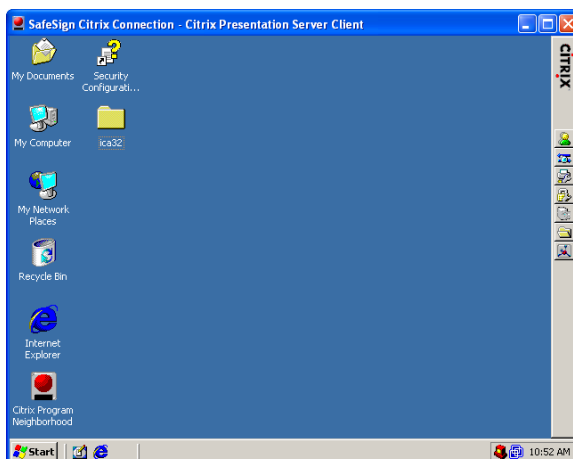


Figure 36: Working Desktop Connection

Congratulations! Your Citrix connection is working with SafeSign Smart Card logon.