

SafeSign Identity Client User Guide

Microsoft Windows Server 2003 Terminal Services

This document contains information of a proprietary nature.

No part of this manual may be reproduced or transmitted in any form or by any means electronic, mechanical or otherwise, including photocopying and recording for any purpose other than the purchaser's personal use 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 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.

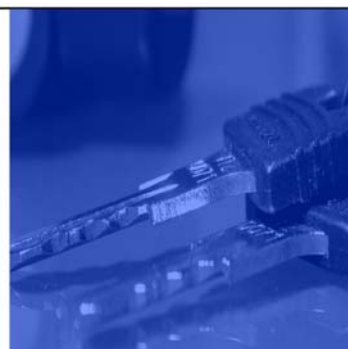
IJsselburcht 3
NL-6825 BS
P.O. Box 5486
NL-6802 EL Arnhem
The Netherlands
Tel. +31-26-365 33 50
Tel. Support +31-26-365 35 43
Fax +31-26-365 33 51



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
Microsoft Windows Server 2003 Terminal Services

Document ID: Windows2003_Terminal_Safesign-IC_v2.1

Project Information: Safesign Identity Client User Documentation

Document revision history

Version	Date	Author	Changes
1.0	14-12-2005	Drs C.M. van Houten	First edition for SafeSign Identity Client Version 2.2 for Windows (release 2.2.0)
1.1	24-04-2006	Drs C.M. van Houten	Edited for SafeSign Identity Client Version 2.2 for Windows (release 2.2.2)
2.0	25-07-2006	Drs C.M. van Houten	Edited for SafeSign Identity Client Version 2.3 for Windows (release 2.3.0)
2.1		Drs C.M. van Houten	Edited for SafeSign Identity Client Version 2.3 for Windows (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
List of Figures	IV
About the Product.....	V
About the Manual	VI
1 Windows 2003 Terminal Services	1
1.1 Prerequisites	1
1.2 Installation of Terminal Server	2
2 Windows Terminal Server Client.....	7
2.1 Deployment	7
2.1.1 Create a client install share	7
2.2 Installation.....	9
3 Using Terminal Services	12
3.1 Set up a Remote Desktop Connection.....	12
3.2 Error messages.....	14
3.2.1 Incorrect PIN	14
3.2.2 Smart card is blocked	14
3.2.3 Keyset does not exist	14
3.2.4 Drivers are not present.....	15
3.3 Logon with protected authentication path devices.....	15
3.3.1 Secure pinpad reader	15
3.3.2 SafeSign Identity Client Bio.....	16
3.4 Use SafeSign Identity Client in a Terminal Session	17
Index of Notes	a

List of Figures

Figure 1: Add Remove Programs	2
Figure 2: Add/Remove Windows Components	2
Figure 3: Windows Components Wizard: Windows Components	3
Figure 4: Windows Components Wizard: Terminal Server setup: install	3
Figure 5: Windows Components Wizard: Terminal Server setup: permissions	4
Figure 6: Configuration Warning: Do you want to continue the installation with these settings?	5
Figure 7: Windows Components Wizard: Configuring Components	5
Figure 8: Windows Components Wizard: Completing the Windows Components Wizard	6
Figure 9: win32 directory	7
Figure 10: win32 Properties: Sharing	8
Figure 11: Remote Desktop Connection – InstallShield Wizard: Welcome	9
Figure 12: Remote Desktop Connection – InstallShield Wizard: License Agreement	10
Figure 13: Remote Desktop Connection – InstallShield Wizard: Customer Information	10
Figure 14: Remote Desktop Connection – InstallShield Wizard: Ready to Install the Program	11
Figure 15: Remote Desktop Connection – InstallShield Wizard: InstallShield Wizard Completed	11
Figure 16: Remote Desktop Connection	12
Figure 17: Remote Desktop Connection: Local Resources	12
Figure 18: Log On to Windows: User name	13
Figure 19: Log On to Windows: PIN	13
Figure 20: Logon Message: An incorrect PIN was presented to the smart card	14
Figure 21: Logon Message: The smart card is blocked	14
Figure 22: Logon Message: The requested keyset does not exist on the smart card	14
Figure 23: Logon Message: The card supplied requires drivers that are not present on this system	15
Figure 24: SafeSign Identity Client GINA: Accessing token	15
Figure 25: SafeSign Identity Client GINA: Secure pinpad reader	16
Figure 29: Remote Desktop: Outlook Express	17

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), 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 SafeNet iKey 3000 USB token with the completed STARCOS SPK 2.3 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), Atmel ATOP36 (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 ID-One Cosmo 64 RSA D/T v5.4 and Oberthur ID-One 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 Ultimate.

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 Microsoft Server 2003 Terminal Services, 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 Windows 2003 Terminal Services.

In order to set up your SafeSign Identity Client Token for use with Microsoft Windows 2003 Server Terminal Services, follow the instructions in the manual.

Every activity has a number of steps, indicated by the numbers at the left-hand side of the text: **1**

Each step will require you to take a certain action, which is indicated by a: ➔

Go through these steps and the actions you are required to take, in order to perform the desired activity,

taking into account the notes in **black** with:  and the larger ones in **blue** with:



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

1 Windows 2003 Terminal Services

Terminal Services is a multi-session environment that gives remote computers access to a server desktop through "thin client" software.

In Terminal Server mode, you can access Windows-based applications or the Windows desktop itself on virtually any computing device - including those that cannot run Windows. When a user runs an application on Terminal Server, 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, Terminal Services allows the same set of applications to run on diverse types of desktop hardware.

Microsoft Terminal Services include Terminal Services Manager and Terminal Services Licensing, administrative tools you can use to manage servers and connections. In addition, Terminal Services includes client software to support Windows-based clients.

An improved feature of Terminal Services in Windows 2003 Server is that it is now possible to log on to the Windows environment using a smart card, as was not possible with previous versions of the Microsoft Terminal Server (Windows 2000 Server did not support smart card services in Terminal Services). A smart card that contains Windows logon credentials can provide those credentials to a Windows Server 2003 remote session for log-on. Note that this feature requires a client OS that can recognize the smart card first: Windows 2000, Windows XP and Windows CE .NET.

1.1 Prerequisites

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

- Active Directory installed and configured;
- Microsoft Certification Authority installed and configured;
- SafeSign Identity Client software installed on the Windows 2003 (Terminal) Server;
- Drivers for the smart card reader(s) installed on the Windows 2003 (Terminal) Server and 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 or Windows Server 2003 used as a client to connect to the Windows 2003 (Terminal) Server.

1.2 Installation of Terminal Server

Microsoft Windows Terminal Server enables users to run Windows-based applications on a remote computer running one of the Windows Server 2003 family of Operating Systems.

Microsoft Terminal Server is part of Microsoft Server 2003, but may have to be installed. Installation of Terminal Server on the server is described below.

1

To install Microsoft Terminal Server, go to **Start -> Settings -> Control Panel** and double click '**Add or Remove Programs**' to open the *Add or Remove Programs* window:

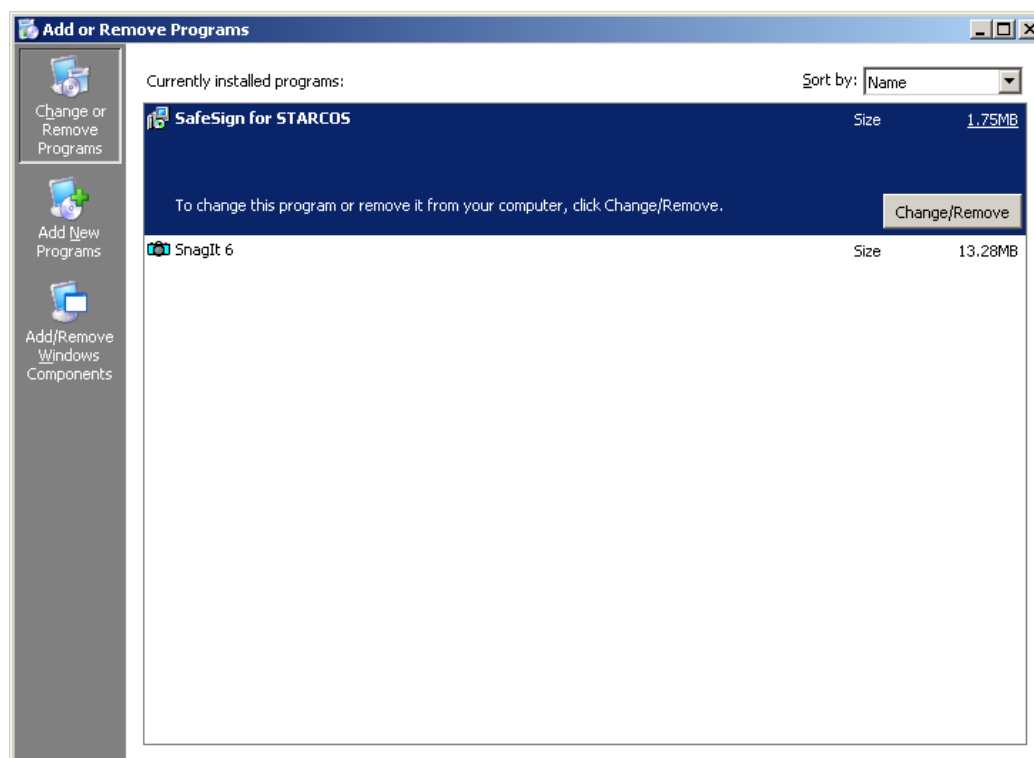


Figure 1: Add Remove Programs

➔ From the **Add or Remove Programs** console double-click **Add/Remove Windows Components**:

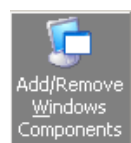


Figure 2: Add/Remove Windows Components

2

This will open the *Windows Components Wizard*, allowing you to check whether or not the Terminal Server is installed:

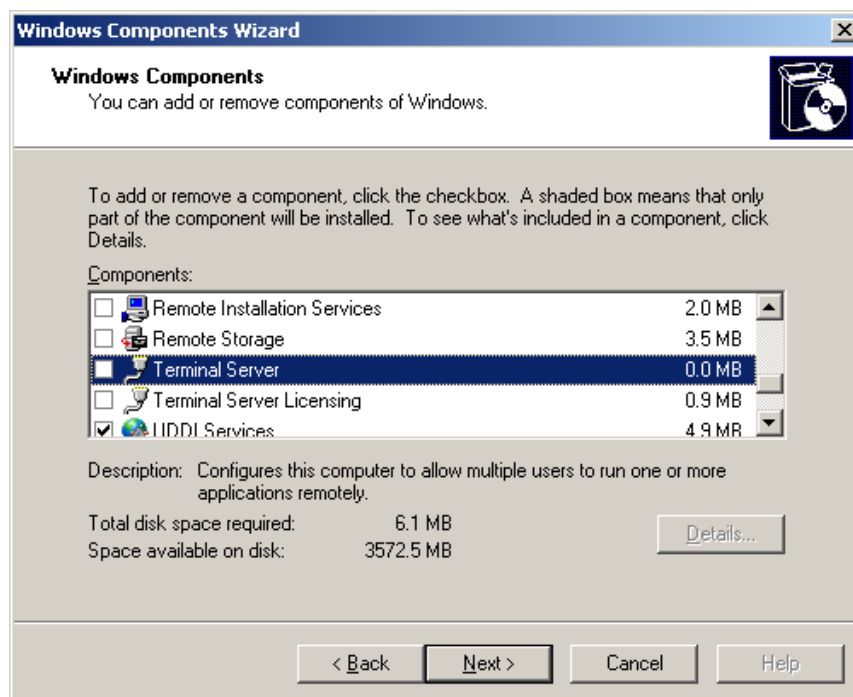


Figure 3: Windows Components Wizard: Windows Components

If the checkbox in front of **Terminal Server** is not checked (as above), Terminal Server is not yet installed.

➔ Check **Terminal Server** and click **Next** to continue

3

The *Terminal Server setup* dialog will appear, displaying the Terminal Server installation notes:

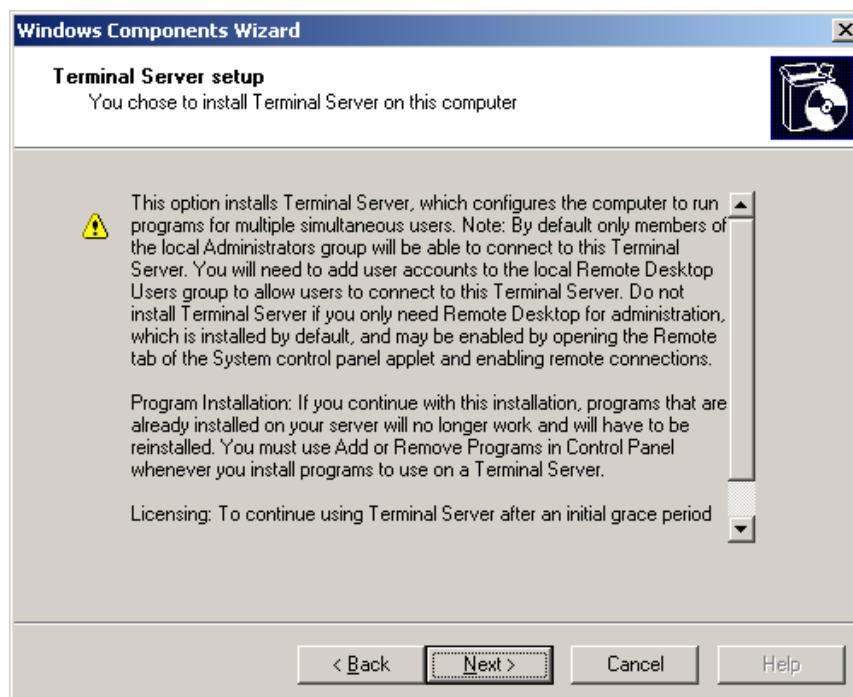


Figure 4: Windows Components Wizard: Terminal Server setup: install

Read the Terminal Server installation notes displayed carefully before continuing. Whether or not you need **Terminal Server Licensing** depends on how you are going to deploy the Terminal Server. Please check the Microsoft site <http://www.microsoft.com/windowsserver2003/howtobuy/licensing/ts2003.msp> whether or not you need to install the Terminal Server Licensing component.

➔ Click **Next** to continue

4

The *Terminal Server setup: Select default permissions for application compatibility* dialog will appear, allowing you to select which security profile is applicable in your situation:

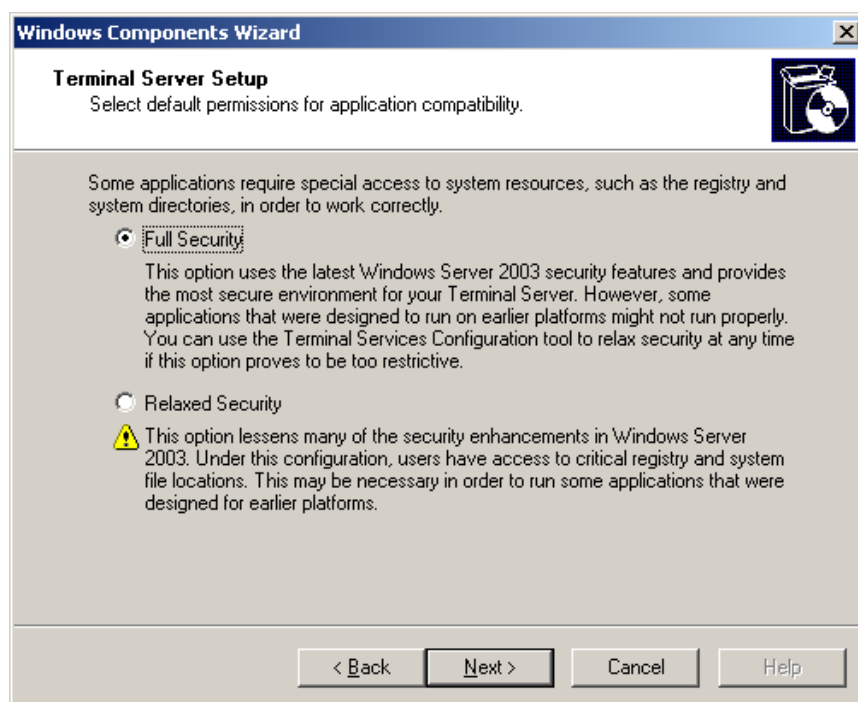


Figure 5: Windows Components Wizard: Terminal Server setup: permissions

➔ Select an option (in this guide, the **Full Security** option is selected) and click **Next** to continue

5

The *Configuration Warning* dialog will appear, informing you about the consequences of the permissions set above (Figure 5) and asking you if you want to continue the installation with these settings:

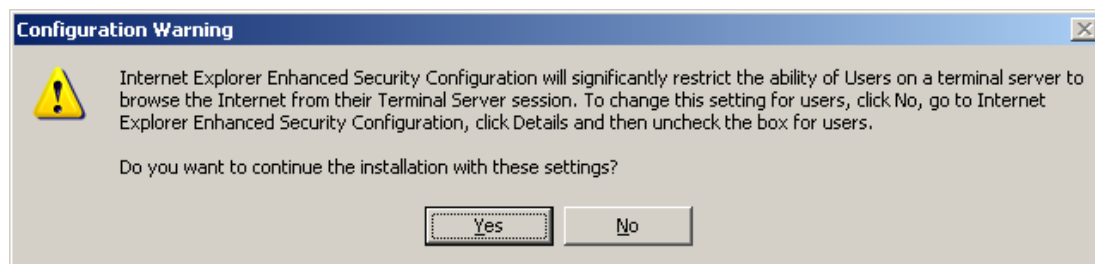


Figure 6: Configuration Warning: Do you want to continue the installation with these settings?

➔ Click **Yes** to continue

6

Upon clicking **Yes**, installation of the Microsoft Terminal Server will proceed:

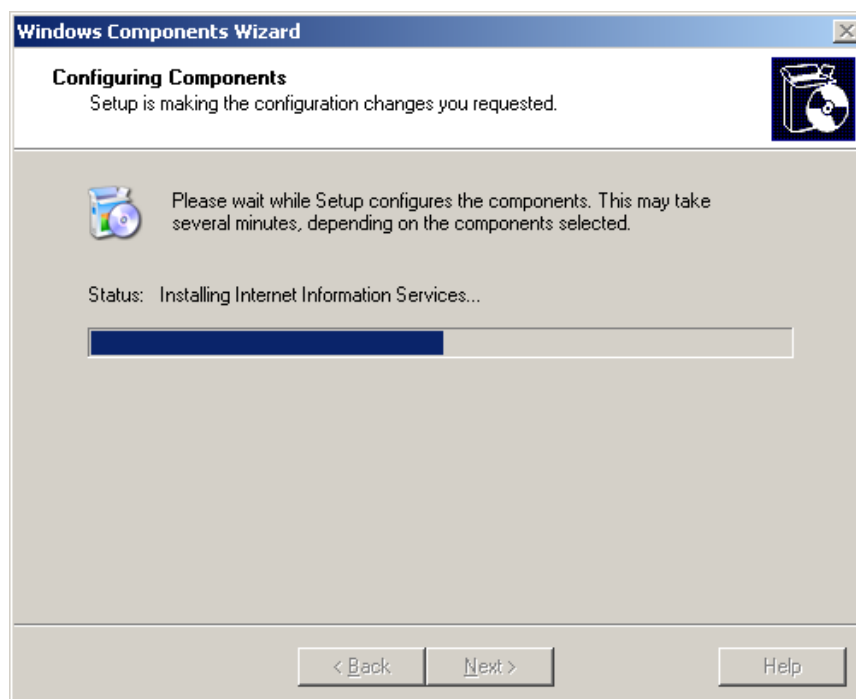


Figure 7: Windows Components Wizard: Configuring Components

➔ Wait until Setup configures the components

7

When Setup has finished configuring and installing the components, the *Completing the Windows Components Wizard* dialog will appear:



Figure 8: Windows Components Wizard: Completing the Windows Components Wizard

- ➔ Click **Finish** to close the Windows Components Wizard

Windows Terminal Server is now installed (on the Windows 2003 Server machine that will act as the Terminal Server). You can now install the Terminal Server Client (Remote Desktop Connection) on the client computers (as described in Chapter 2).

2 Windows Terminal Server Client

2.1 Deployment

For a client to connect to the Terminal Server, it is necessary to install the Terminal Server Client, called the **Remote Desktop Connection** (application).

Remote Desktop Connection is built into Windows XP and Windows Server 2003. For client computers that do not have Remote Desktop Connection installed, but want to do so, one of the following options may be used:

- Use tools such as Microsoft Systems Management Server or Windows 2000 Group Policy to publish / assign the Windows Installer-based Remote Desktop Connection.
- Create a client install share on Windows Server 2003. (This can also be done on Windows 2000 Server.)
- Install directly from the Windows XP or Windows Server 2003 CD, using the 'Perform Additional Tasks' selection from the CD's autoplay menu. (**Note** This does not require installing the operating system.)
- Download the Remote Desktop Connection from <http://www.microsoft.com/windowsxp/using/mobility/getstarted/remoteclient.mspix>

In this guide, we will describe how to create a client install share on the Windows Server 2003.

2.1.1 Create a client install share

For deployment convenience it could be useful to share the installation source of the Remote Desktop Connection application so that it can be easily installed from a different computer.

The installation source of the Remote Desktop Connection application is installed during the installation of the Terminal Server component in the following directory:

<windows installation drive>:\<windows installation path>\system32\clients\tsclient\win32

Open the directory

<windows installation drive>:\<windows installation path>\system32\clients\tsclient\win32

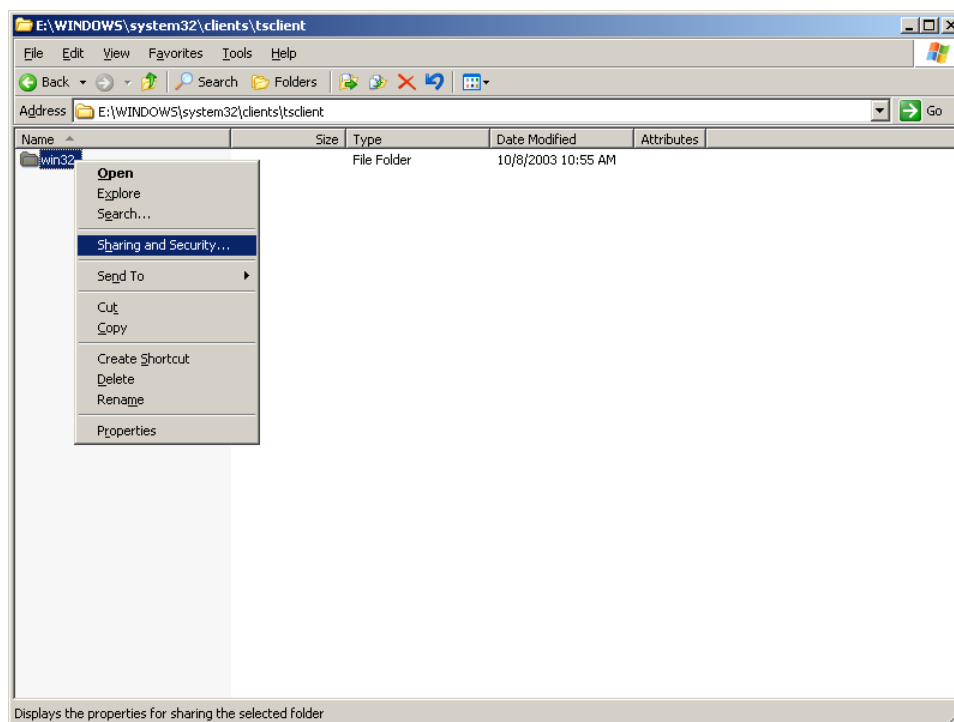


Figure 9: win32 directory

➔ Right-click on the directory you wish to share and select **Sharing and Security** (as above)

The *Properties* dialog for the folder will appear, with the tab **Sharing** opened:

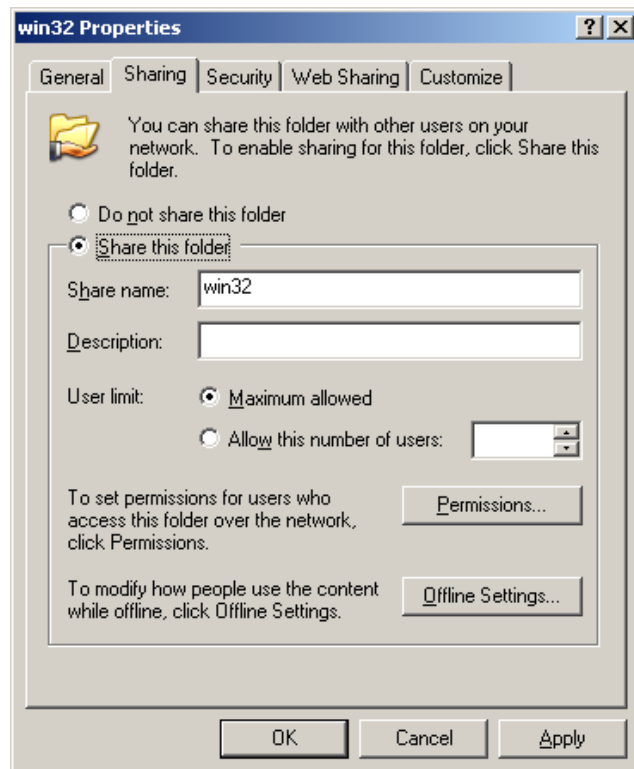



Figure 10: win32 Properties: Sharing

➔ Select **Share this folder** (as above) and then click **OK**

The win32 directory is now shared, as indicated by the hand through the directory , and can now be reached from a different computer.

2.2 Installation

As described above, the Remote Desktop Connection application can be installed by creating a client install share on the Terminal Server, which can be reached by the client by connecting to the shared directory. In this shared directory will be the Remote Desktop Connection application source that has to be installed in order to connect to the Terminal Server.

1

Go to the shared directory where the Remote Desktop Connection application source can be found, i.e. `<terminalserver_name>\win32` and double-click *setup.exe* to start the *Remote Desktop Connection InstallShield Wizard*.

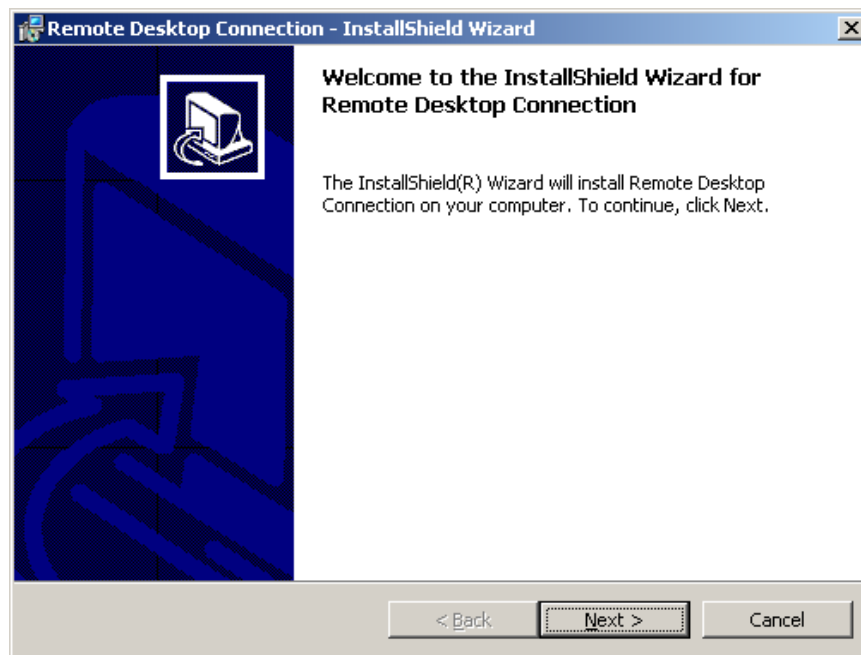


Figure 11: Remote Desktop Connection – InstallShield Wizard: Welcome

➔ Click **Next** to continue

2

Upon clicking **Next**, the *License Agreement* dialog will be displayed:

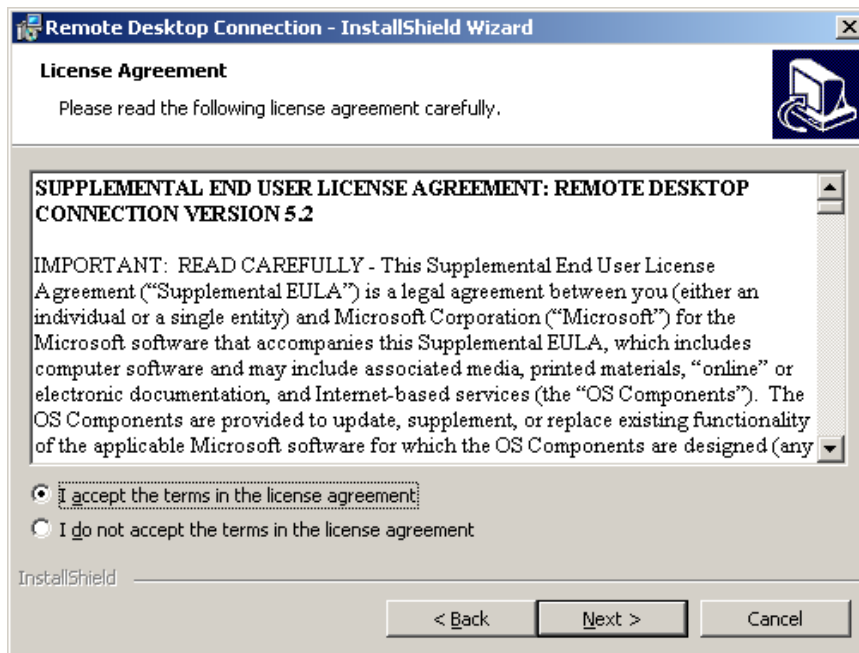


Figure 12: Remote Desktop Connection – InstallShield Wizard: License Agreement

- ➔ If you agree with the license agreement select **I accept the terms in the license agreement** and click **Next** to continue

3

The *Customer Information* dialog allows you to fill in your information:

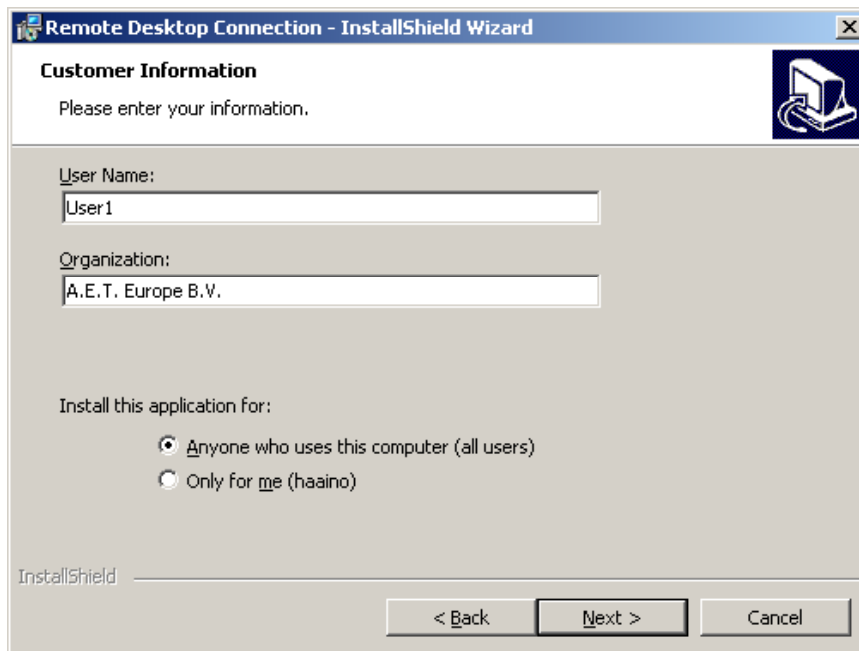


Figure 13: Remote Desktop Connection – InstallShield Wizard: Customer Information

- ➔ Enter the requested details and click **Next** to continue

4

After filling in all the required installation details, the installation of the Remote Desktop Connection application is ready to begin:

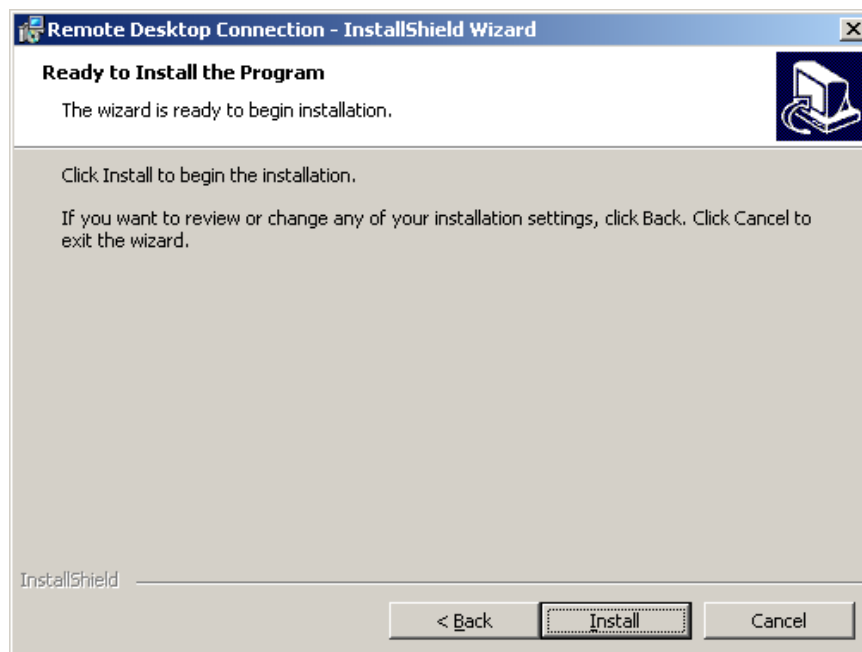


Figure 14: Remote Desktop Connection – InstallShield Wizard: Ready to Install the Program

➔ Click **Install** to install the Remote Desktop Connection application

5

When the Remote Desktop Connection application has been installed, you will be informed in the *InstallShield Wizard Completed* dialog:

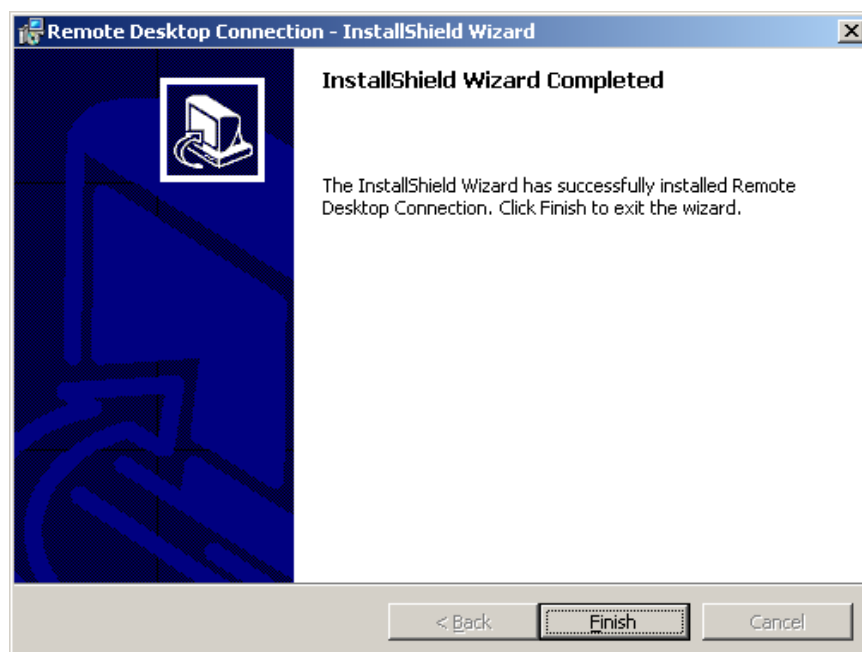


Figure 15: Remote Desktop Connection – InstallShield Wizard: InstallShield Wizard Completed

➔ Click **Finish** to exit the wizard

Remote Desktop Connection is now installed. If the Windows Server 2003 has been set up as Terminal Server, you can now set up a connection (as described in Chapter 3).

3 Using Terminal Services

3.1 Set up a Remote Desktop Connection

With the Remote Desktop Connection (application) installed on the client, you can connect to a Windows 2003 Terminal Server.

Start the Remote Desktop Connection by going to **Start -> Programs -> Remote Desktop Connection**:

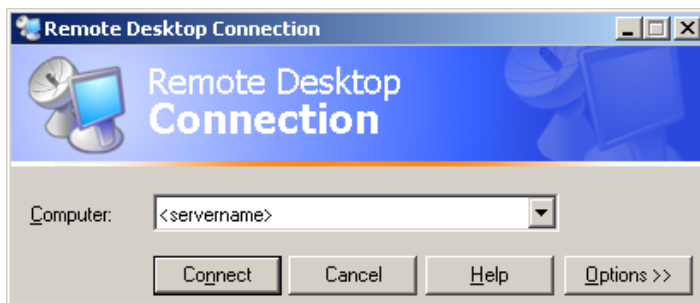


Figure 16: Remote Desktop Connection

➔ Enter the computer name of the Terminal Server

When you have started the Remote Desktop Connection application, before connecting, you should first verify the local device connection settings, in particular, if the smart card (installed on the client) is connected to when logged on to the remote computer.

In order to do so, click **Options** (in [Figure 16](#)) and open the tab **Local Resources**:



Figure 17: Remote Desktop Connection: Local Resources

➔ Verify if under *Local devices*, the option **Smart cards**¹ is checked and if not, select it

¹ This option will be available when a smart card reader is installed on the local computer.

You can now connect to the Terminal Server by clicking **Connect**, after which the *Log On to Windows* dialog will appear, asking you for a user name and password, if the token is not yet inserted:

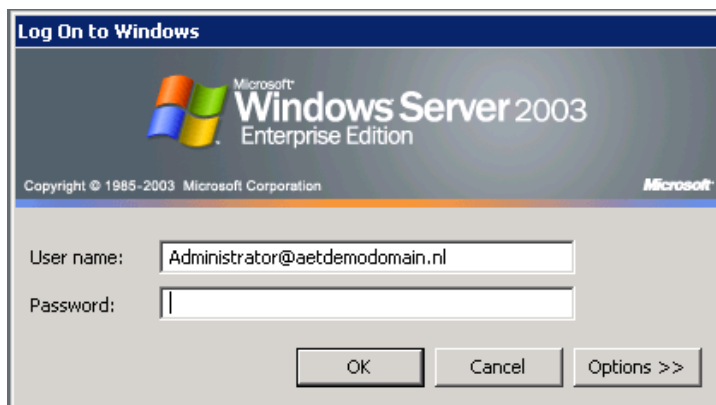


Figure 18: Log On to Windows: User name

- ➔ Insert your SafeSign Identity Client token (containing a smart card login certificate for the domain)

Upon inserting your SafeSign Identity Client token (or if your token is already inserted upon clicking **Connect**), the *Log On to Windows* dialog will appear, asking you for a PIN:



Figure 19: Log On to Windows: PIN

- ➔ Enter the PIN for your SafeSign Identity Client Token and click **OK**

After you have entered the (correct) PIN, you will be logged on to the Terminal Server.

3.2 Error messages

The following (*"the system could not log you on"*) error messages may appear when connecting to a remote desktop.

3.2.1 Incorrect PIN

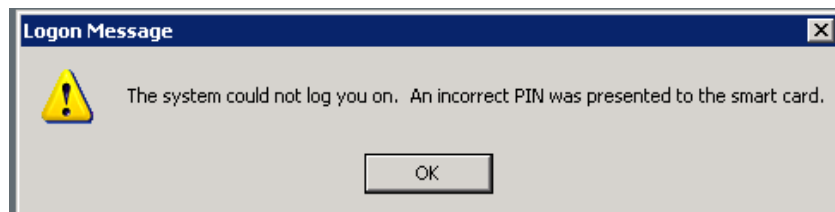


Figure 20: Logon Message: An incorrect PIN was presented to the smart card

- ➔ The PIN you entered for the token is incorrect

3.2.2 Smart card is blocked

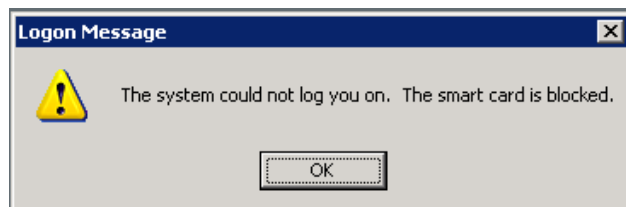


Figure 21: Logon Message: The smart card is blocked

- ➔ The PIN of the token is locked. Use the Token Utilities to unlock the PIN.

3.2.3 Keyset does not exist

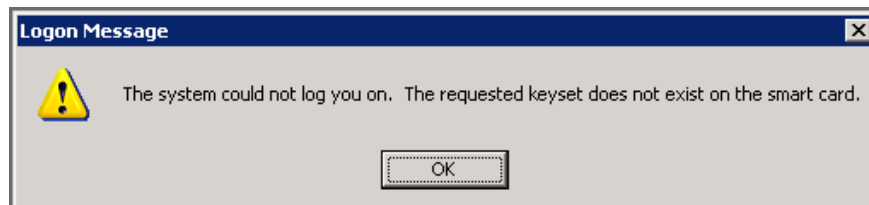


Figure 22: Logon Message: The requested keyset does not exist on the smart card

- ➔ The token is either (a) an uninitialised ('blank token'), or (b) does not contain a (correct) certificate. Use the Token Utilities to initialise your token and/or verify that it does contain a (correct) certificate.

3.2.4 Drivers are not present



Figure 23: Logon Message: The card supplied requires drivers that are not present on this system

- ➔ This error may be caused by the fact that SafeSign Identity Client is not installed on the Terminal Server or that you have inserted an unknown / unsupported token. Use the Token Utilities to verify that the token is recognised. If it is not recognised ('unknown token'), an administrator may use the Token Administration Utility to create a registry file (with the option *Query unknown token*) to add the token (when the token is listed as supported in the Product Description).

3.3 Logon with protected authentication path devices

3.3.1 Secure pinpad reader

When you have a secure pinpad reader, you should not enter the PIN of your SafeSign Identity Client token in the PIN dialog that Windows presents upon card insertion ([Figure 19](#)). Rather, you should use the keypad of your secure pinpad reader.

SafeSign Identity Client facilitates this for you, when you have installed the SafeSign Identity Client GINA¹.



Note

Note that for Windows 2003 Terminal Server, you need to install SafeSign Identity Client including the GINA on the Terminal Server. The description below assumes that you have done so:

After inserting your token (or when it is inserted), wait to be prompted to enter your PIN on the secure pinpad reader:

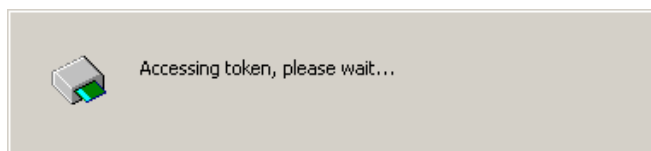


Figure 24: SafeSign Identity Client GINA: Accessing token

You will then be prompted by your secure pinpad reader when to enter the PIN on its keypad, either by a message on the display of your secure pinpad reader or by a blinking LED. Note that the way this is done, is determined by the secure pinpad reader and cannot be influenced by SafeSign Identity Client.

¹ For the installation of the GINA, refer to the installation guide. It will be not installed by default. If you want to install the GINA, you will need to select it during installation. Note that if you do not install the GINA, the secure pinpad reader functionality is supported (see Note 'SafeSign GINA not installed' on the next page).



SafeSign Identity Client GINA not installed

When the SafeSign Identity Client GINA is not installed on the server, but it is installed on the client, you will need to click **OK** or press **Enter** at the to logon prompt (Figure 19), to have the following dialog appear and have the secure pinpad reader prompt you for the PIN of your SafeSign Identity Client Token:

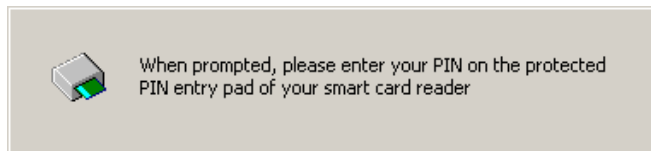


Figure 25: SafeSign Identity Client GINA: Secure pinpad reader

The same applies when you do not have installed the GINA (on the client) at all.

3.3.2 SafeSign Identity Client Bio

When you have SafeSign Identity Client Bio installed, the same applies with regard to the use of a secure pinpad reader (i.e. you should enter the PIN on the keypad of the secure pinpad reader) as described in paragraph 3.3.1. Moreover, the *Authentication* dialog will be displayed, showing a picture of the secure pinpad you are using.

When you SafeSign Identity Client Bio installed and are using a G&D StarSign® BioToken 3.0, you can authenticate using your fingerprint.

3.4 Use SafeSign Identity Client in a Terminal Session

When logged in with your smart card on the Terminal Server, you can use all applications available with your SafeSign Identity Client Token (just as you would on your PC, when not working in a terminal server session).

For example, you can send a signed e-mail message with Outlook Express:

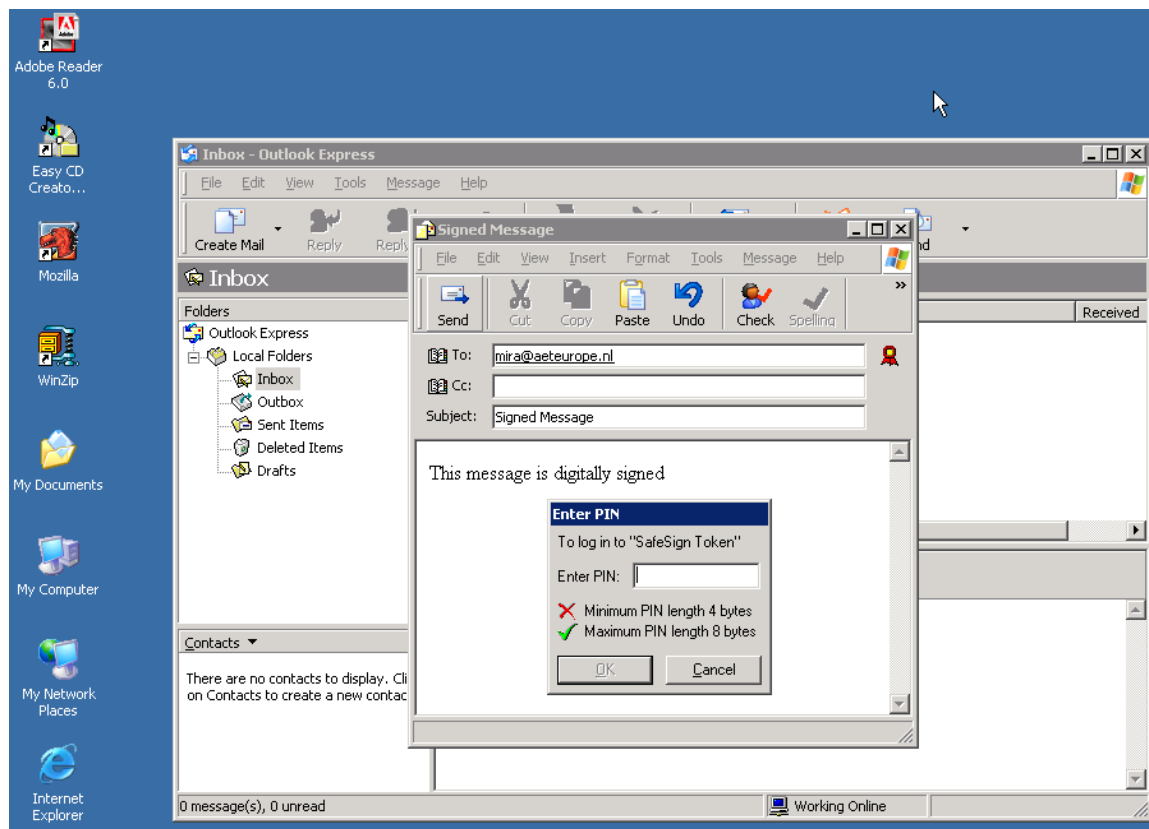


Figure 26: Remote Desktop: Outlook Express



Remove Token

When you remove your token, the Remote Desktop Connection may be locked or disconnected (logged off), depending on the setting of the Domain Controller Security Policy for smart card removal behaviour.

Index of Notes

Logon Message	14
Note	15
Remove Token	17
SafeSign GINA not installed	16