Certificate Rollout Whitepaper

Table of Contents

Introduction

The Microdasys SCIP-Proxy uses its own Root CA for each defined SCIP Account. The Root CA is either the default Microdasys Root CA Certificate or a customized Root CA created through the Web-Interface or a already existing imported CA. To prevent the Web-Browser from prompting that the presented Web-Certificate is not trusted, the Microdasys Root-CA-Certificate needs to be imported into the List of trusted CA's.

Manual Root CA Import

Get the Root CA

You need to download the root certificate and install it into your browser. This can be done by using an import Wizard in most browsers.
The location of the Root CA in SCIP depends on the Account that is used. In the default case the Certificate is located here:
Windows:
`%PROGRAMDIR%\Microdasys\Sx Suite\Program\conf\CA_default\PCA\`
Linux/Solaris:
`/opt/sxsuite/conf/CA_default/PCA/`
The name of the Cert file is: `PCAcert.der`

To make it available through a Web-Browser you need to copy the file to the conf/html Folder.
Give the following Link to your users:
http://internala.microdasys.scip/command/file?PCAcert.der

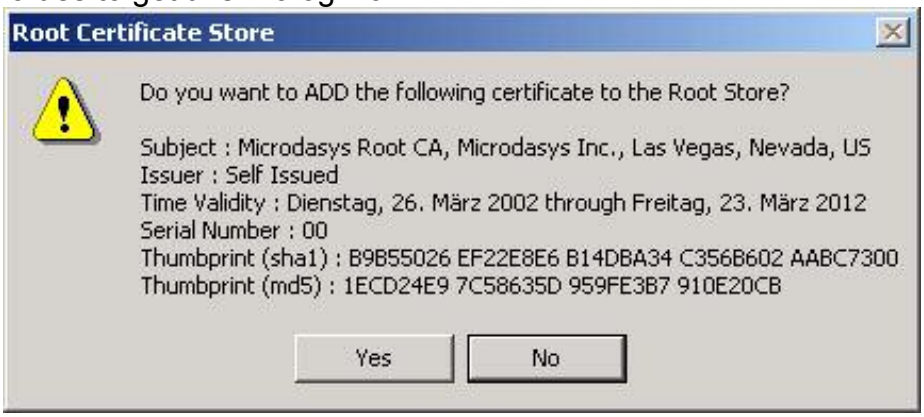
Alternatively you can place this file on an Intranet-Webserver.

The Process of trusting a CA-Certificate is implemented differently in each Browser. Here are some screenshots that will illustrate the process for the most common Web-Browsers.

Internet Explorer 5.0, 5.5,6.0

You should enter “Open this file from its current location” in the first screen:

A Mouse-Click on „Install Certificate“ will initiate the Installation-Process. Just accept the default-values to get this Dialog-Box:



By clicking “Yes”, the Microdasys Root-CA is accepted as trusted and the Microdasys SCIP-Proxy works now completely transparent for the end user.

Netscape Navigator 4.7

The Root-CA Import with the Netscape Navigator is quite long. But you only have to accept the default-values except for one second Picture you will see here.

Attention: Now you have to click on the first checkbox to make the Navigator accept the Microdasys Root CA-Certificate for Certifying network sites.

Now you can type in any name you want.

Done...

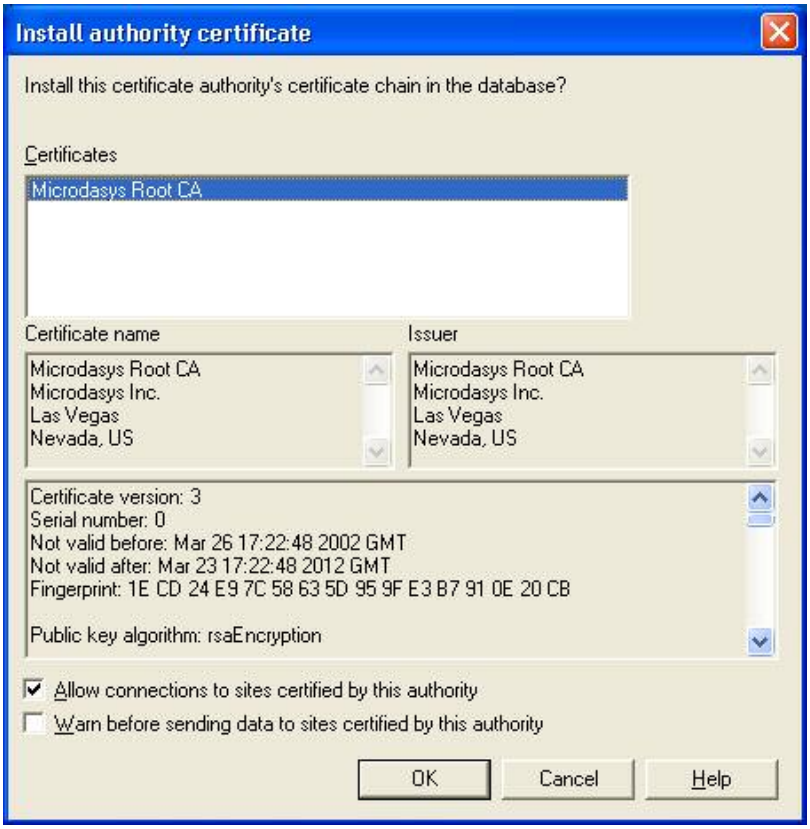
Netscape 6/7

The Import-Process in Netscape 6/7 is one of the shortest.

You see something similar to this Screenshot and **you just have to check the first Checkbox and click on “OK”.**

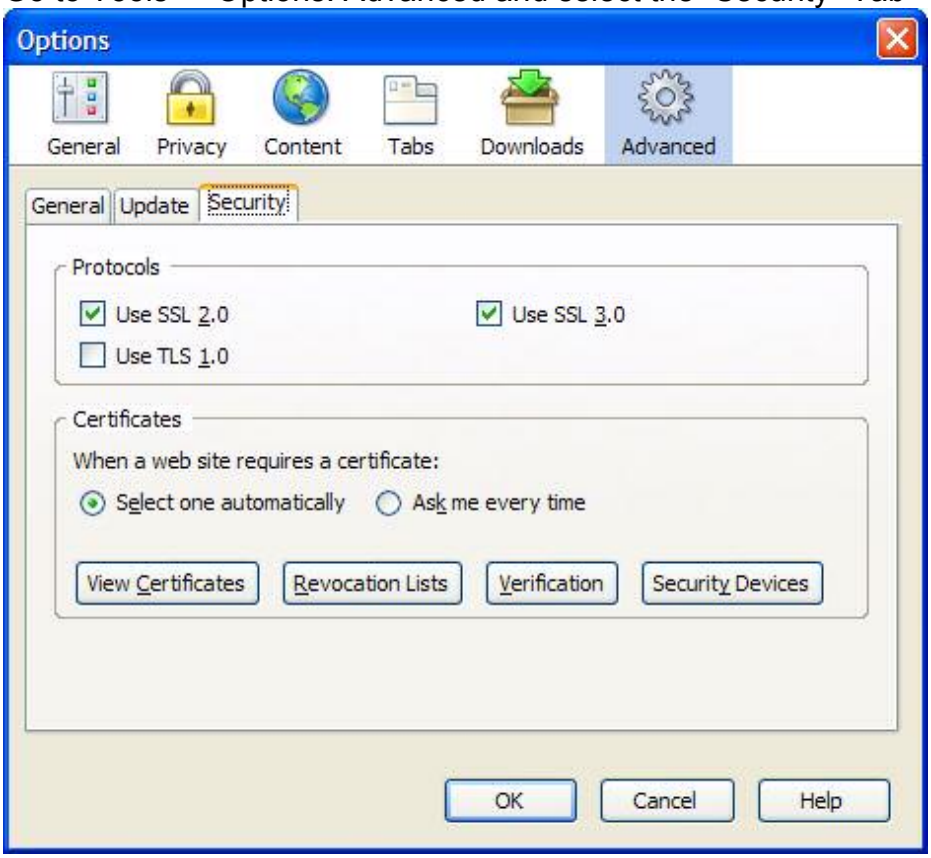
Opera 6

The Import-Process in Opera 6 is the shortest. Just press “OK” in the following Dialog-Box.

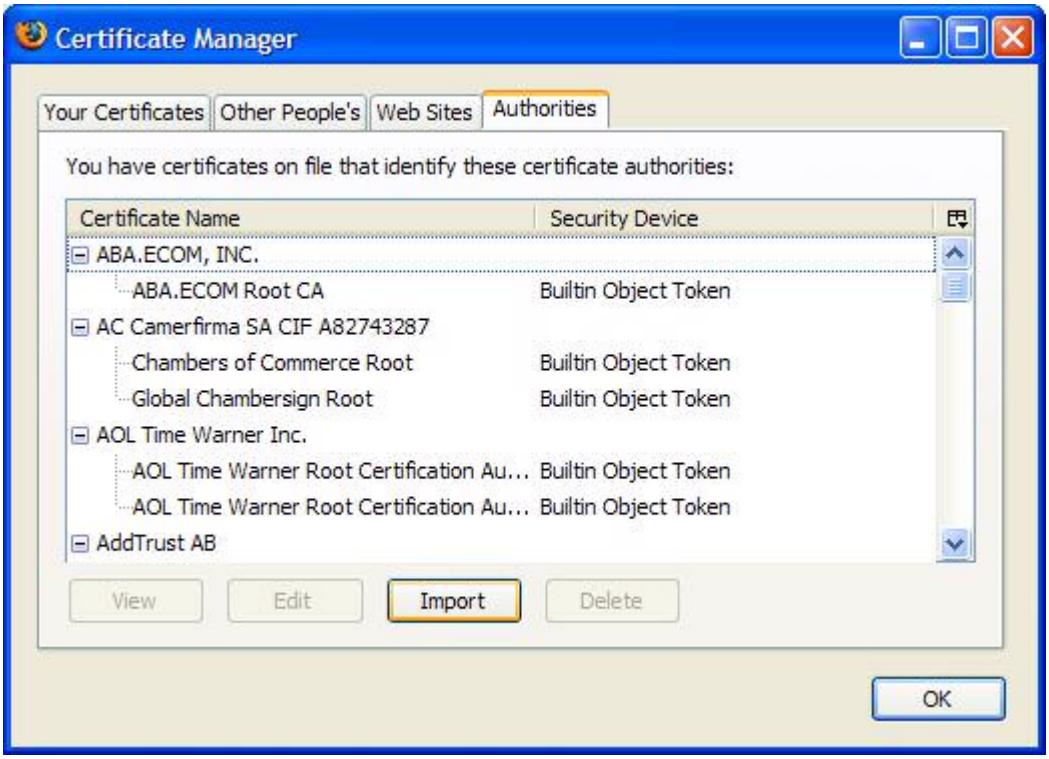


Firefox 1.5

Go to Tools -> Options: Advanced and select the “Security”-Tab

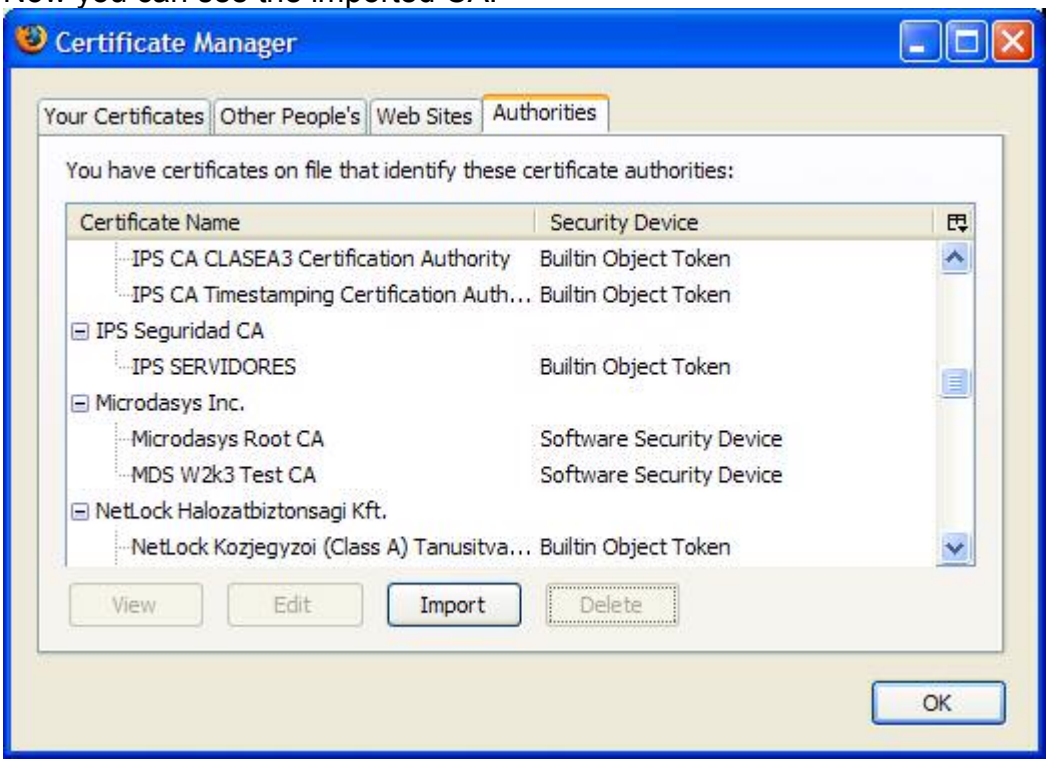


Choose “View Certificates” and select the “Authorities”-Tab



Select “Import” and browse the PCAcert.pem file
Check the “Trust this CA to identify web sites.” Box and press OK.

Now you can see the imported CA:



Using the Active Directory for Certificate Rollout

Getting the Microdasys Root CA as a file to Import into the CA Store

The location of the Root CA in SCIP depends on the Account that is used. In the default case the Certificate is located here:

Windows:

```
%PROGRAMDIR%\Microdasys\Sx Suite\Program\conf\CA_default\PCA\
```

Linux/Solaris:

```
/opt/sxsuite/conf/CA_default/PCA/
```

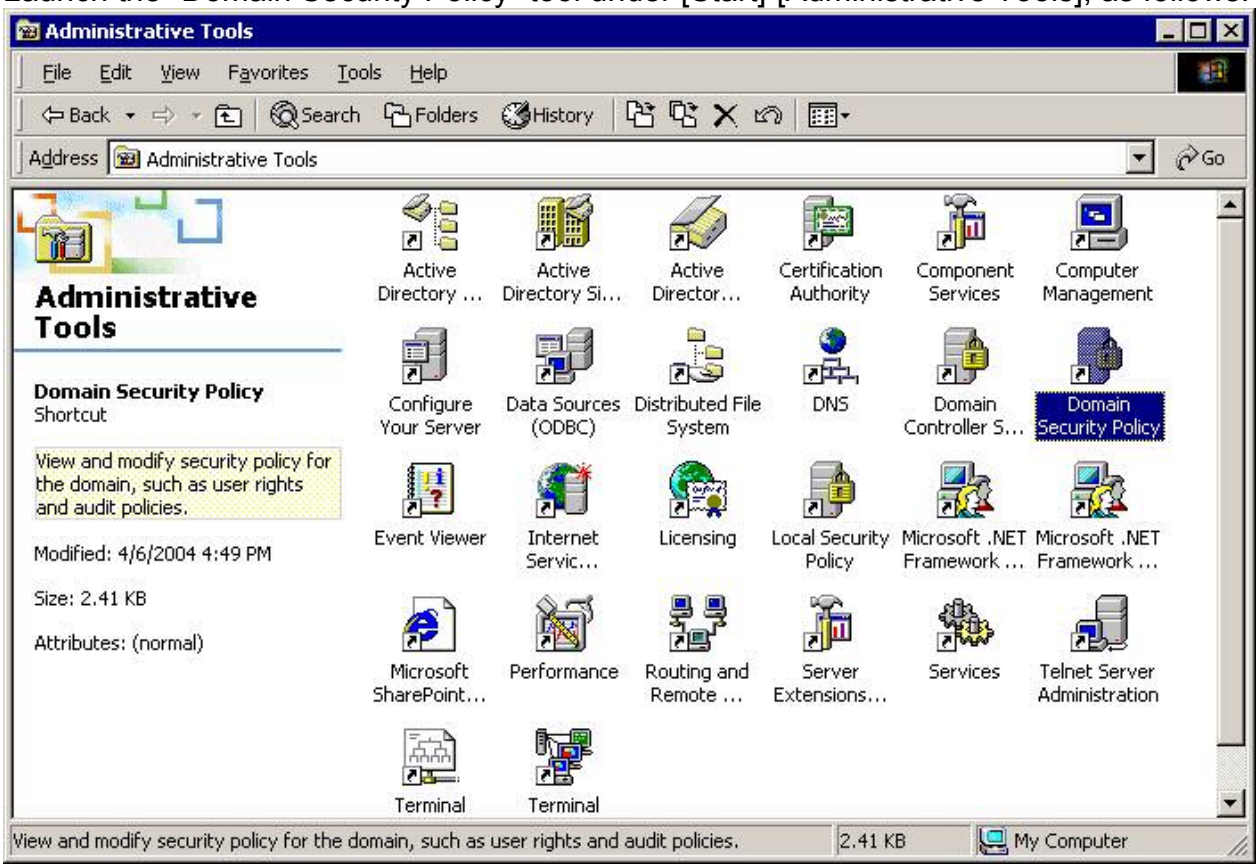
The name of the Cert file is: `PCAcert.der`

You will need this file later when importing it into the Active Directory.

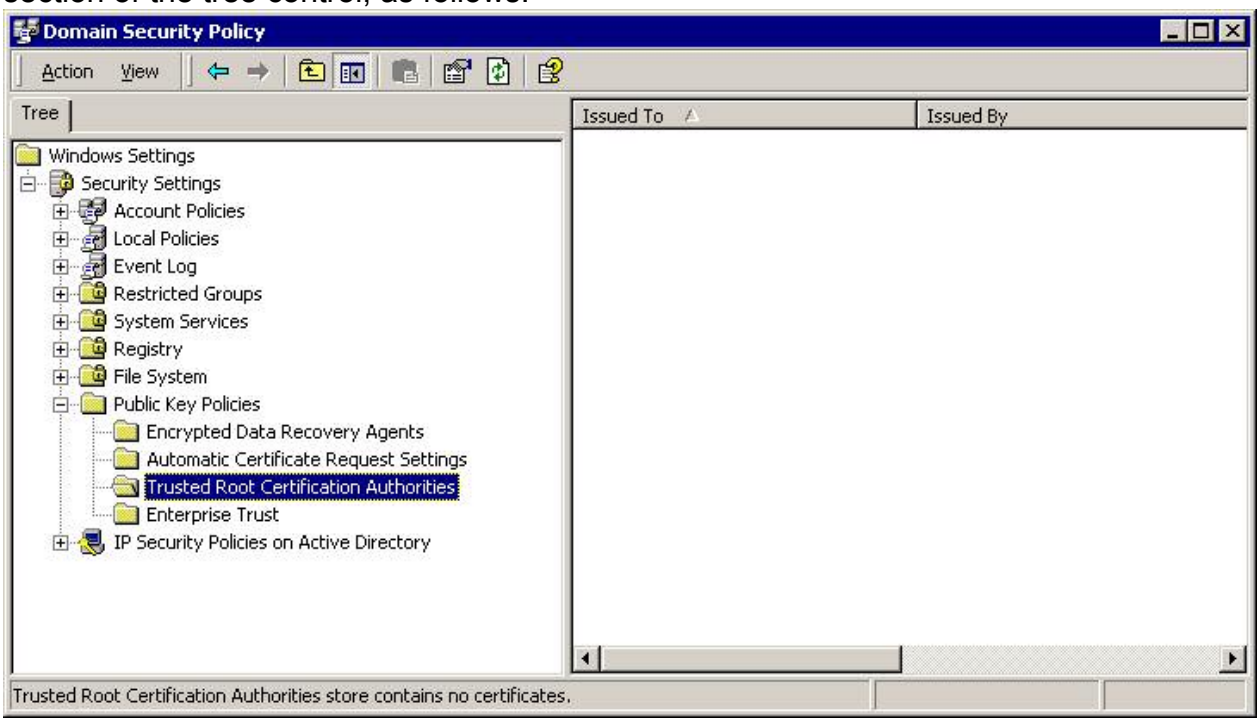
Use Active Directory to Distribute the Microdasys SCIP Root Certificate to Windows 2000 Domain Members

If you are using a homogenous Windows 2000 Active Directory domain environment, you can use the regular Microsoft tools for distributing the Microdasys SCIP Root certificate to Windows 2000 clients that are members of the domain. You must be logged in with Administrative-level privileges to perform these steps. The general idea is to import the Microdasys SCIP Root certificate into the “Default Domain Group Policy”.

Launch the “Domain Security Policy” tool under [Start]-[Administrative Tools], as follows:

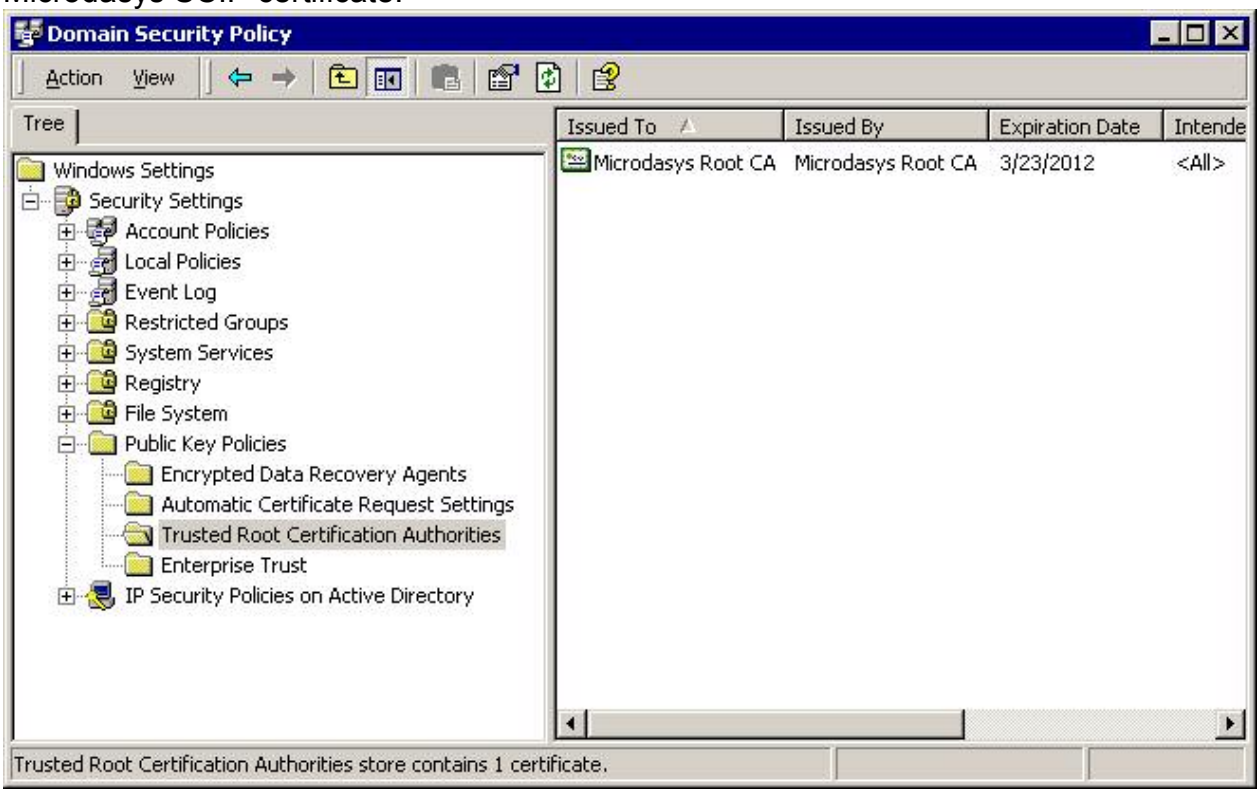


Navigate to the “Trusted Root Certification Authorities” under “Public Key Policies” section of the tree control, as follows:



With the “Trusted Root Certification Authorities” section highlighted, select the [Actions] menu item, and choose “All Tasks”, and “Import”.
The “Import Certificate Wizard” will load. Continue through the Wizard to import the Microdasys SCIP Certificate File.

After the import is complete, the “Domain Security Policy” window should display the Microdasys SCIP certificate:



Windows 2000 clients will import this certificate on the next policy update. If you wish to enforce the
policy update immediately, you may run the following Microsoft tool from the “CMD” command-line:
secedit /refreshpolicy machine_policy /enforce
and:
secedit /refreshpolicy user_policy /enforce
You may wish to check the “Application Event Log” on the computer running “**secedit**” to ensure the
policy update applied successfully. In addition, you may wish to check the “Application Event Log” on
the client computers to verify no errors have occurred.

Manual Certificate Rollout using the command line or login script

Microsoft provides a tool called **CERTMGR.EXE**. If this tool does not already exist on your computer, Microsoft provides it in the Platform SDK (August 2000), which is available on the Microsoft web site:
http://msdn.microsoft.com/library/default.asp?url=/library/enus/security/security/utilities_to_create_view_and_manage_certificates.asp

CERTMGR.EXE also comes in IE4 and IE5 versions, which are available from the Microsoft web site [use the tree control to navigate to Security - Authenticode - Authenticode for IE 4, or IE 5.5]
http://msdn.microsoft.com/downloads/default.asp

If you include **CERTMGR.EXE** to run silently in a login script, the proper command line arguments are as follows:

```
certmgr -add -all -c PCAcert.der -s -r localMachine root
```

No pop-up dialogs will be produced by this tool, and the certificate will install silently.

The location of the Root CA in SCIP depends on the Account that is used. In the default case the Certificate is located here:
Windows:
`%PROGRAMDIR%\Microdasys\Sx Suite\Program\conf\CA_default\PCA\`
Linux/Solaris:
`/opt/sxsuite/conf/CA_default/PCA/`
The name of the Cert file is: `PCAcert.der`

You may verify that the Microdasys Root CA certificate is properly imported by viewing the Certificate Store using Internet Explorer [Tools] - [Options] - [Content] - [Certificates] on client machines.