

Implementing Gemalto Smart Card for Use with HP Compaq t5720 and HP CCI



Introduction	2
Prerequisites	2
Reference hardware and software	3
Reference Documents	4
Installing GemSafe Libraries 5.0 SE to Server and Client PCs (Optional)	5
Installing Microsoft Certificate Services	9
Configuring a Certificate Authority (CA) service	13
Configuring Microsoft Certificate Authority to Issue Smart Card User Certificate	18
Manually issue Smart Card User Certificate	24
Testing the Smart Card	27
Creating Customized User Install Packages for Clients PCs (Optional)	30
Additional Information	36
Using a Smart Card For Windows Network Login	36
Administration of the GemSafe Smart Card	36
Working with GemSafe Libraries	36
Usage cases	37
Usage case 1: User authentication from blade PC to Active Directory Domain	37
Usage case 2: User authentication from client device to blade PC or Active Directory Server using RDP	38
Usage case 3: User authentication from client device to blade PC or Active Directory Server using HPSAM client	38
Usage case 4: Accessing secure Web site	39
Usage case 5: User authentication using VPN through firewall to blade PC or Active Directory Server	40
Usage case 6: User authentication from client device using Citrix server	43
Service and Support	45

Introduction

Smart cards can provide additional security to a corporate network. This paper provides instructions for configuring a smart card with your HP Compaq t5720 thin client and CCI blade PCs.

Gemalto delivers secure personal devices, software, and services through innovation and collaboration—thus, enabling our clients to offer trusted and convenient digital services to billions of individuals. A key component of these solutions is the smart card where Gemalto Smart cards solutions are considered a secure, reliable and easy to use identification credential for corporate enterprise. Smart cards are considered a secure, reliable, and easy to use identification credential for corporate enterprise.

The corporate enterprise requires secure access to network resources from their Information Technology Departments. IT Departments must provide authentication solutions that employees can use without creating undo time or effort. Gemalto and Hewlett Packard have combined their network access solutions to deliver both security and ease of use. Replacing the outdated and easy to hack “user name and password” authentication method, corporate employees can log onto corporate resources via HP thin clients using the Gemalto GemXpresso Identification Card. While the employee needs only to remember a simple password, the GemXpresso ID Card protects the employee’s identity with an advanced cryptographic key without sacrificing log-on time. Along with secure access, the Gemalto GemXpresso ID Card can provide additional applications such as physical access control, digital signature certificates, VPN authentication and disk/file encryption.

Instructions for deploying the GemSafe Libraries, SmartCard readers drivers to Thin Client, Thick Client, CCI Blade or SAM server, in addition environmental network infrastructures such as Windows 2003 Server setup for DHCP, DNS, Active Directory, IIS including CCI SAM and Load Balancers is beyond the scope of this white paper; therefore, the white paper assumes the customer has acknowledged RDP enablement settings at both server and client, firewall settings are appended as necessary, and usage of the Enhanced Write Filter are already functional and comprehended for usage and configuration.

For further information about purchasing Gemalto products, including the GemSafeXpresso 3.2 Java cards or GemSafe libraries, please send an e-mail to Gemalto at HP@Gemalto.com, or call 888-343-5773.

Prerequisites

1. GemSafe Libraries v5.0 SE or GemSafe Libraries v5.1 SE (Vista).
2. Gemalto Java Cards:
 - GemSafeXpresso 32k v. 3.2 Java cards.
 - GemSafeXpresso 64k v. 3.2 Java cards.
3. Before installing GemSafe Libraries you must connect the smart card reader.
 - a. Connect your reader.
 - To connect the HP USB SmartCard Keyboard, plug the keyboard into an available USB Port on your PC.
 - To connect the GemPC Serial-SL, or GemPC Twin Serial:
 - Plug the green cable connector into the serial port on the PC.



- Plug the keyboard cable into the grey extension socket.
- Plug the purple connector of the reader into the keyboard port of the PC.
- To connect the GemPC Card insert the reader into an available PCMCIA slot.

b. Install your reader driver.

The identified Gemalto supported cards are managed within the Gemalto libraries 5.0 SE software installation. For the drivers update, visit the Gemalto support site at: <http://hotline.gemalto.com/>

For the HP USB SmartCard Keyboard Drivers please visit www.hp.com software support for the latest available drivers.

NOTE: GemSafe Libraries 5.0 SE Registration tool found in the system tray inappropriately identifies "no card reader detected". The software continues to operate normally and no user impact occurs. Start and stop the Registration tool using the 'right-click' menu options to resolve the reader identification issue. For more details regarding the operation of the Registration tool, consult the GemSafe user guide.

Reference hardware and software

The following list provides the reference hardware and software used to validate the Gemalto Smartcard with the identified Usage cases:

- Load Balancer
 - HP Server running F5 networks BigIP version 4.6.4.
 - or
 - HP Server running HP Session Allocation Manager version 1.0.
- Primary Domain Controller
 - HP server running Microsoft Windows Enterprise 2003 Server RC1. Configured as DNS, DHCP, IIS, CA, and secure Web site server.
- VPN Tunnel
- Altiris Deployment Server
- Network Switch.
 - HP Procurve 2626.
- Blade Enclosure
 - HP e-class blade enclosure.
- Blade PCs
 - HP bc1000 blade PC running Microsoft Windows XP SP2 w/HPSAM blade service installed.
 - HP bc1500 blade PC running Microsoft Windows XP SP2 w/HPSAM blade service installed.
- Clients



- HP Compaq t5720 series thin client running Microsoft Windows XPe w/HPSAM blade service installed.
- HP desktop PC running Microsoft Windows XP w/HPSAM blade service installed.
- Smart Card Readers
 - HP standard USB Smart Card Keyboard.
Driver: HPKBCCID.sys, version 4.30.0.1.
 - USB CAC approved smart card reader (SCM Microsystems SCR331 Reader).
Driver: SCR33X2K.sys, version 4.27.00.01.
 - Serial CAC approved smart card reader (SCM Microsystems SCR131 Reader).
 - USB Combo Fingerprint & Smart Card reader (SCM Microsystems SPR337).
Driver: spr337.sys, version 1.16.00.01.
- Gemalto reader support, as follows:

Product	Description	Part Numbers
GemPC Twin (USB)	GemPC Twin Smart Card Reader with USB cable	HWP108765
GemPC Twin (Serial)	GemPC Twin Smart Card Reader with RS232 cable	HWP108925
GemPC USB –SL	USB Smart Card Reader Slim Line Casing	HWP108841
GemPC Serial –SL	Serial Smart Card Reader Slim Line Casing	HWP108927
GemPC Card (PCMCIA)	PC Card Smart Card Reader	HWP110628

- Windows Enterprise 2003 Server RC1.
 - Configured as DNS, DHCP, IIS, CA and secure Web site server.
 - IIS installed.
- Administrative privileges to the server.
- Know the common name for Microsoft Certificate Authority to be defined during the CA installation.

Reference Documents

For more information about HP Consolidated Client Infrastructure, see <http://h71028.www7.hp.com/enterprise/cache/9885-0-0-225-121.html>.

For more information about write filter usage, see the Using the Enhanced Write Filter white paper at: <http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00101105/c00101105.pdf>.



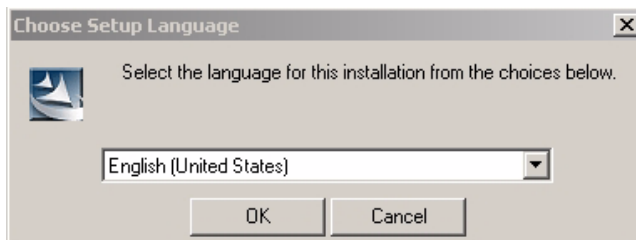
Installing GemSafe Libraries 5.0 SE to Server and Client PCs (Optional)

Running the GemSafe Libraries 5.0 SE on a server or client for card provisioning is required. It is optional to install GemSafe Libraries 5.0 SE to client systems for user logon. The client install package is customizable and created by the Administrator (see **“Creating Customized User Install Packages for Clients PCs (Optional)” on page 30**).

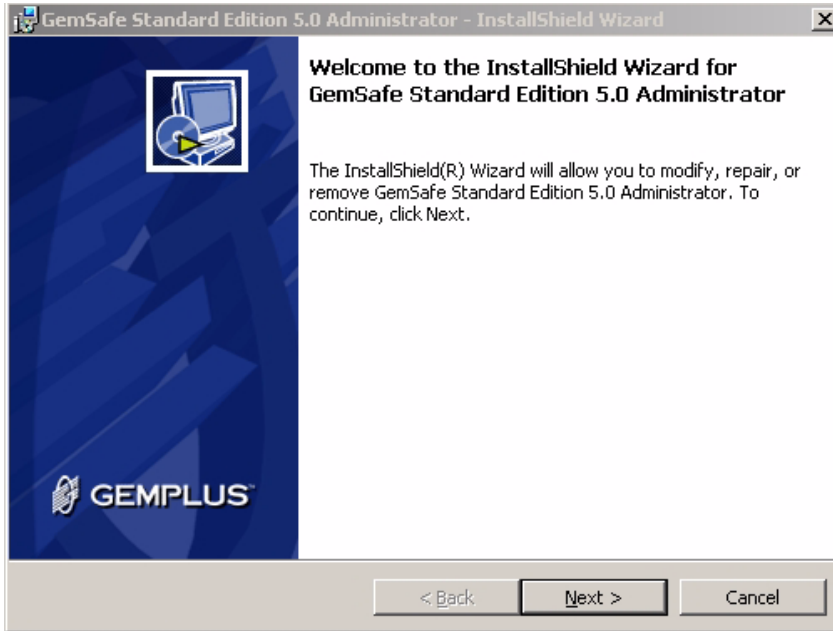
NOTE: During the software installation the reader should not have a smart card in it.

NOTE: Thin Client PC Ram disk size may need to be adjusted up to 64-MB, and changes to the environmental variables will be required for the optional GemSafe Libraries 5.0 SE installation or customized user install packages on an HP Thin Client. For more information see **“Creating Customized User Install Packages for Clients PCs (Optional)” on page 30**.

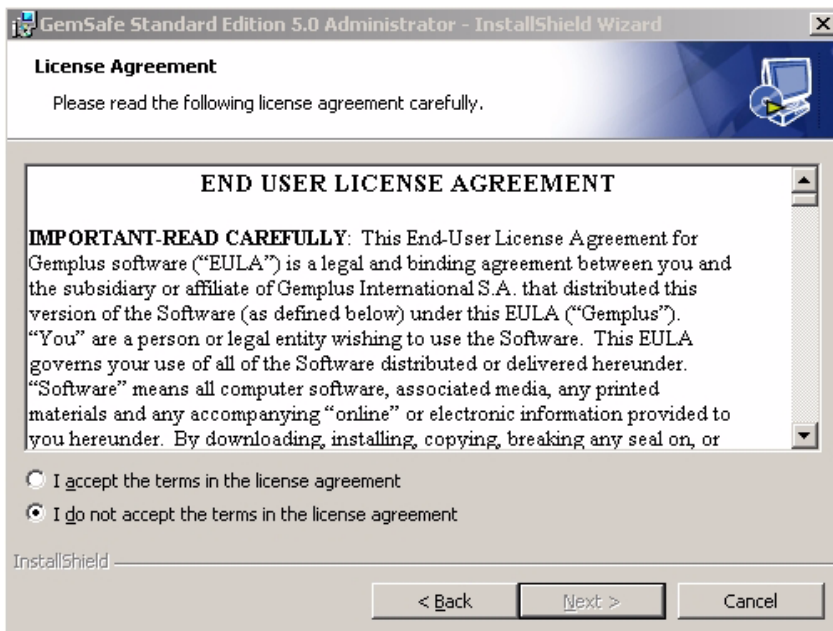
1. Close all opened Windows programs and applications.
2. For Server installation, insert the GemSafe Libraries 5.0 SE CD.
3. The installation program will start automatically if the computer is configured to "autorun" a CD. If your computer is not configured this way, navigate to the CD and double click on the file 'Autorun.exe'.
4. The GemSafe Libraries InstallShield Wizard displays the Autorun window.
5. Select the language of your choice and click **Install** to continue.



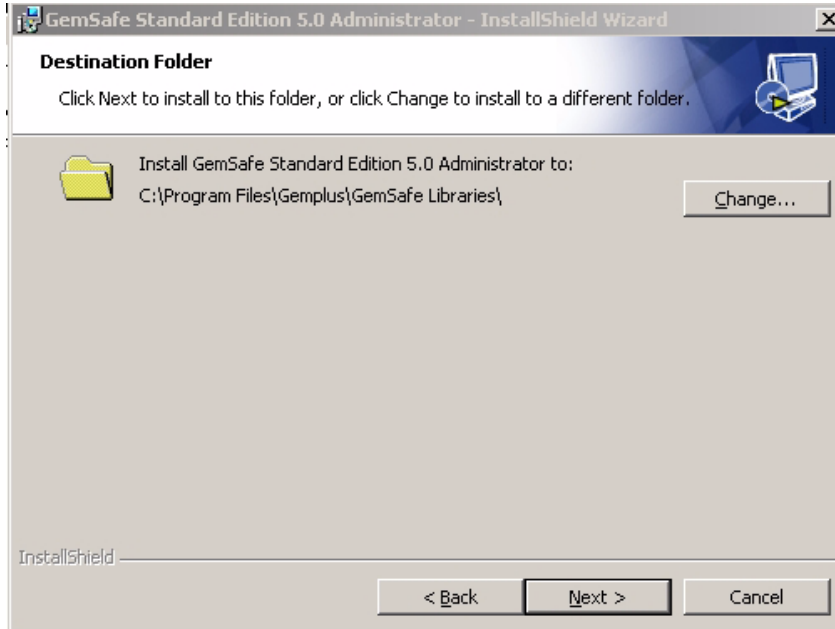
6. Click **Next** to continue; GemSafe Libraries Install Shield Wizard displays the License Agreement window.



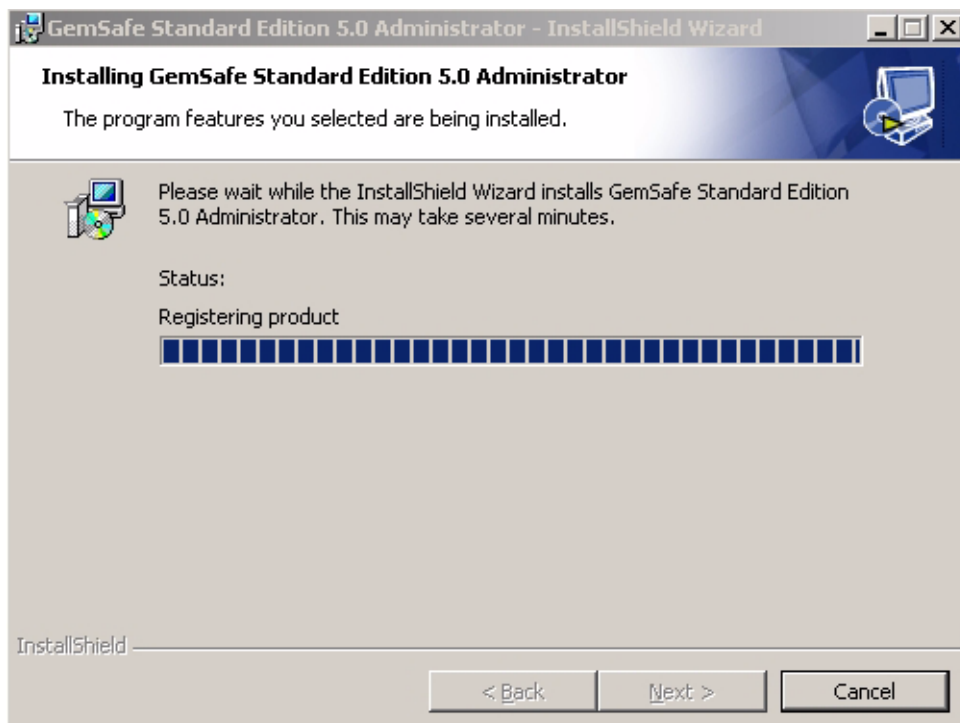
7. Read the Gemalto License Agreement and click **Yes** to continue; the GemSafe Libraries InstallShield Wizard displays the Choose Destination Location window.



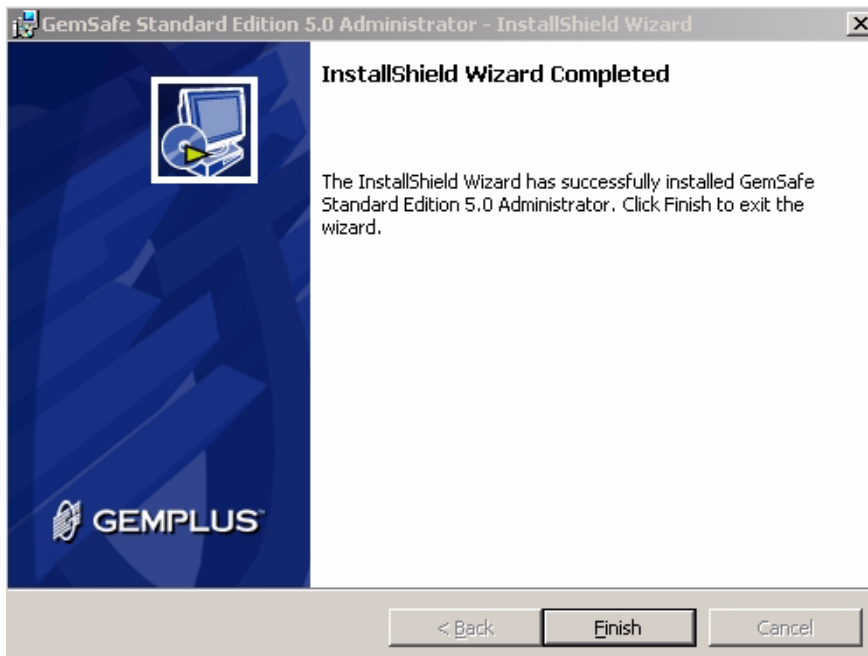
8. Click **Next** to install GemSafe Libraries to the default location or select a different location by using the **Browse** button.



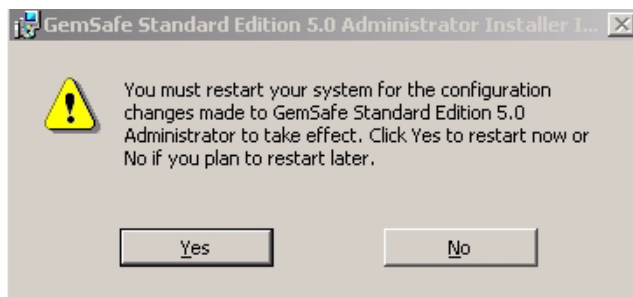
During the GemSafe Libraries installation you will see a series of dialogs similar to the following. These dialogs simply inform you as each of the components are automatically being installed.



9. Click **Finish** to complete the installation; the GemSafe Libraries InstallShield Wizard displays the Reboot Dialog.



10. Click **Yes** to restart the system immediately or **No** to restart your computer later.



NOTE: To use GemSafe Libraries you must restart the computer.

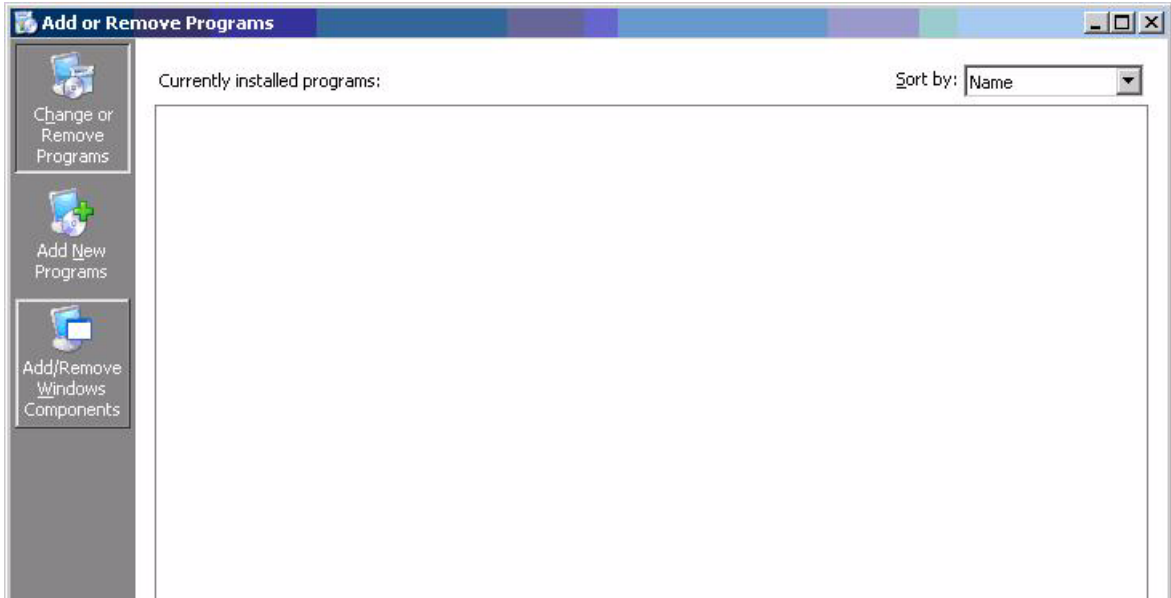
NOTE: Internet Explorer is automatically configured to work with GemSafe Libraries. For the Netscape Security Module configuration please refer to the Administration or User Guide.

NOTE: If you are using the smart card for network login, it will be necessary to load a certificate onto the card in order to recognize the card for login purposes. Instructions for manually issuing a certificate on the card, can be found at ["Manually issue Smart Card User Certificate" on page 24](#).

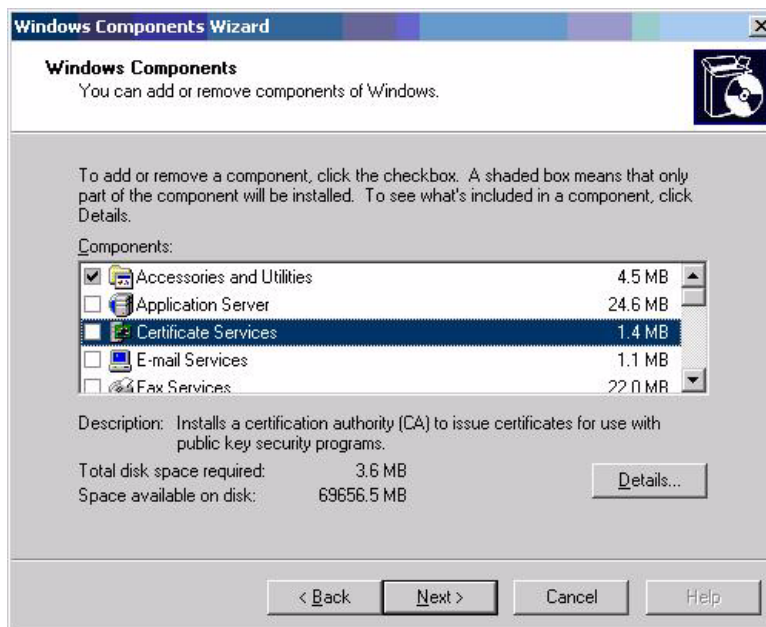
NOTE: After installation of GemSafe Libraries the Administrator has to create users setups by granting users different access rights for GemSafe card management based on their privileges.

Installing Microsoft Certificate Services

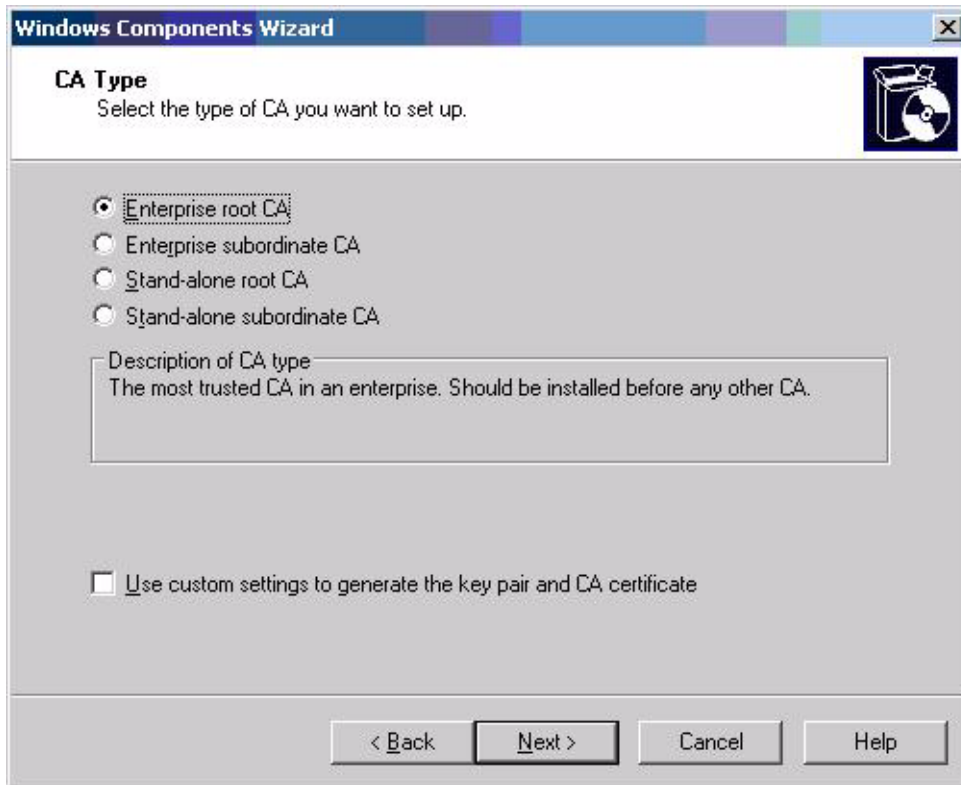
1. Click **Start > Control Panel**.
2. Select **Add or Remove Programs**.
3. In the left panel, select **Add/Remove Windows Components**.



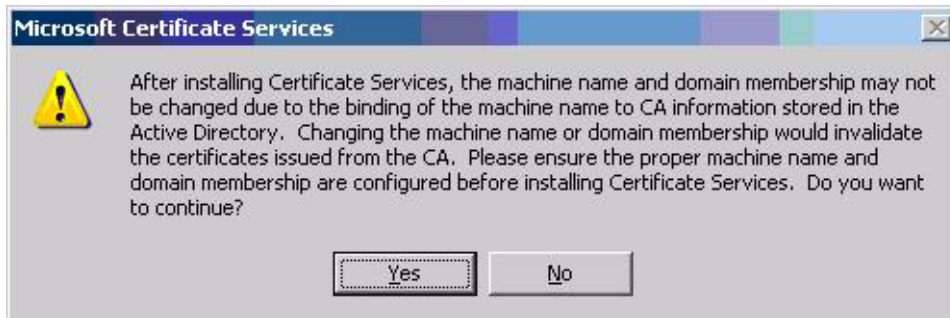
4. Click **Certificate Services**, and then click **Next**.



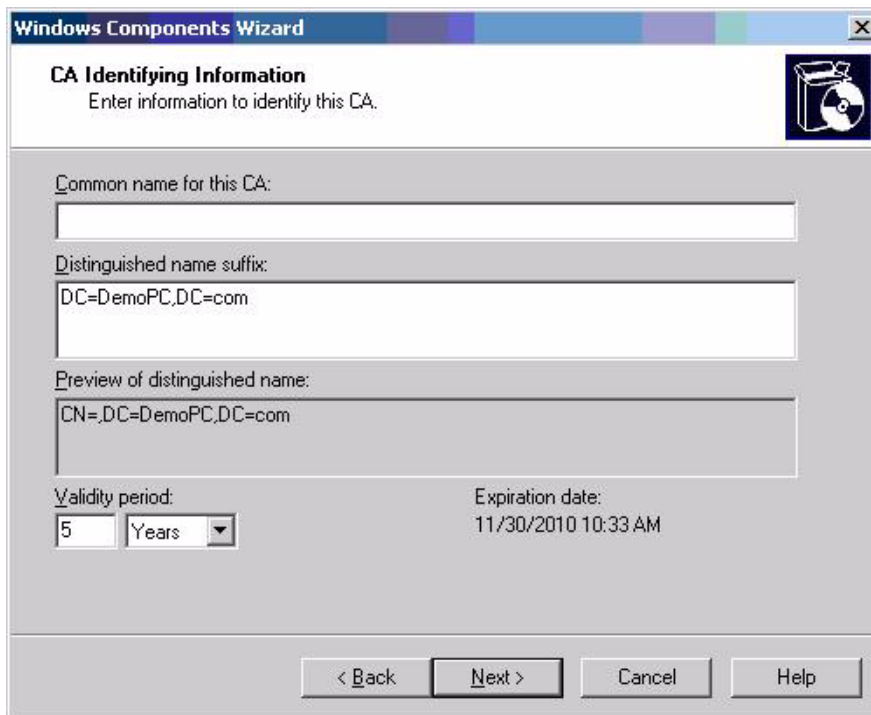
5. Select **Enterprise Root CA**, and then click **Next**.



6. Click **Yes** to accept the warning.

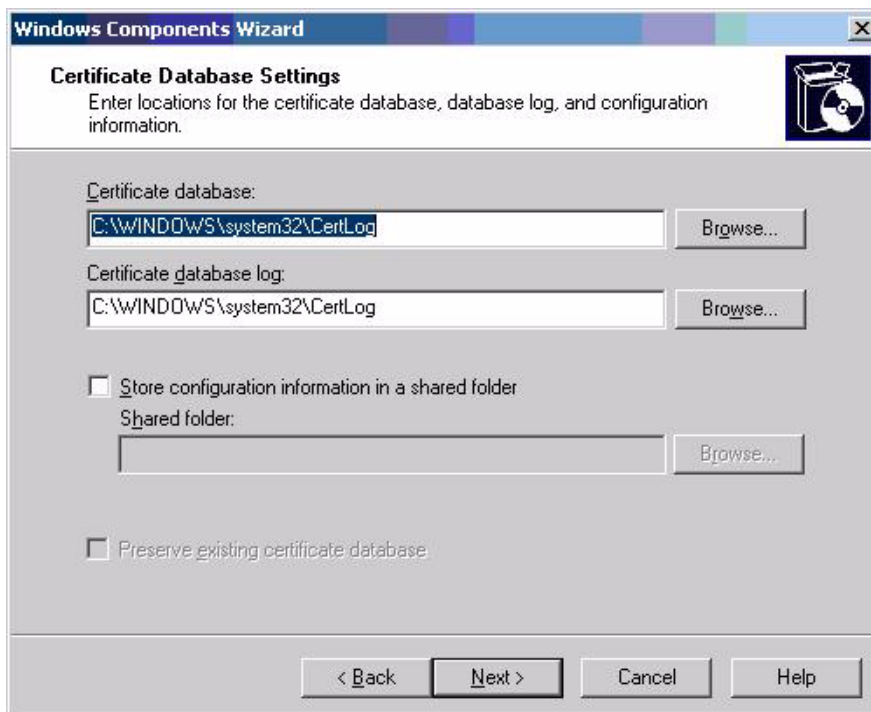


7. Type a **Common name for this CA**, and then click **Next**.



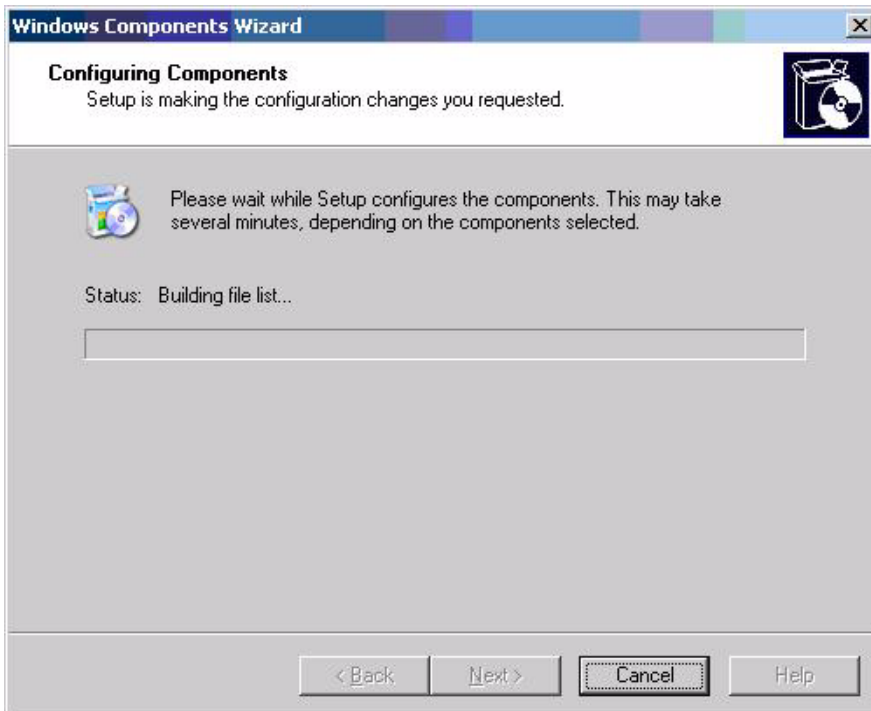
The screenshot shows the 'CA Identifying Information' dialog box in the Windows Components Wizard. The title bar reads 'Windows Components Wizard'. The main title is 'CA Identifying Information' with the subtitle 'Enter information to identify this CA.' Below the title bar, there are four input fields: 'Common name for this CA:' (empty), 'Distinguished name suffix:' (containing 'DC=DemoPC,DC=com'), 'Preview of distinguished name:' (containing 'CN=,DC=DemoPC,DC=com'), and 'Validity period:' (set to '5' years). To the right, the 'Expiration date:' is '11/30/2010 10:33 AM'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

8. Select **Next** to accept Certificate Database Settings.

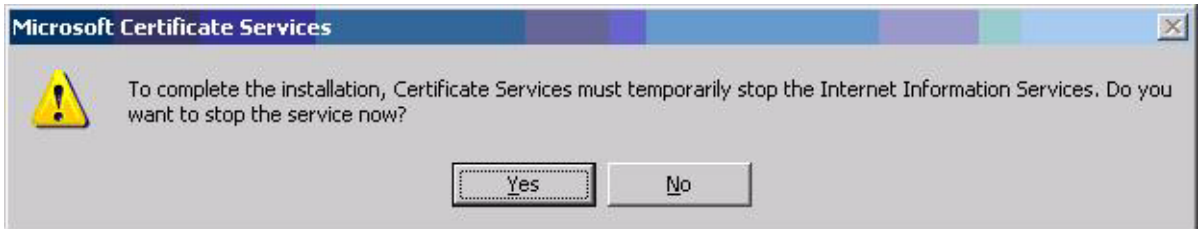


The screenshot shows the 'Certificate Database Settings' dialog box in the Windows Components Wizard. The title bar reads 'Windows Components Wizard'. The main title is 'Certificate Database Settings' with the subtitle 'Enter locations for the certificate database, database log, and configuration information.' Below the title bar, there are three input fields with 'Browse...' buttons: 'Certificate database:' (containing 'C:\WINDOWS\system32\CertLog'), 'Certificate database log:' (containing 'C:\WINDOWS\system32\CertLog'), and 'Shared folder:' (empty). There are two checkboxes: 'Store configuration information in a shared folder' (unchecked) and 'Preserve existing certificate database' (unchecked). At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

The installation will configure components, as shown in the following screen.



9. Click **Yes** when prompted to temporarily stop ISS.



10. Click **Finish** to complete the installation.



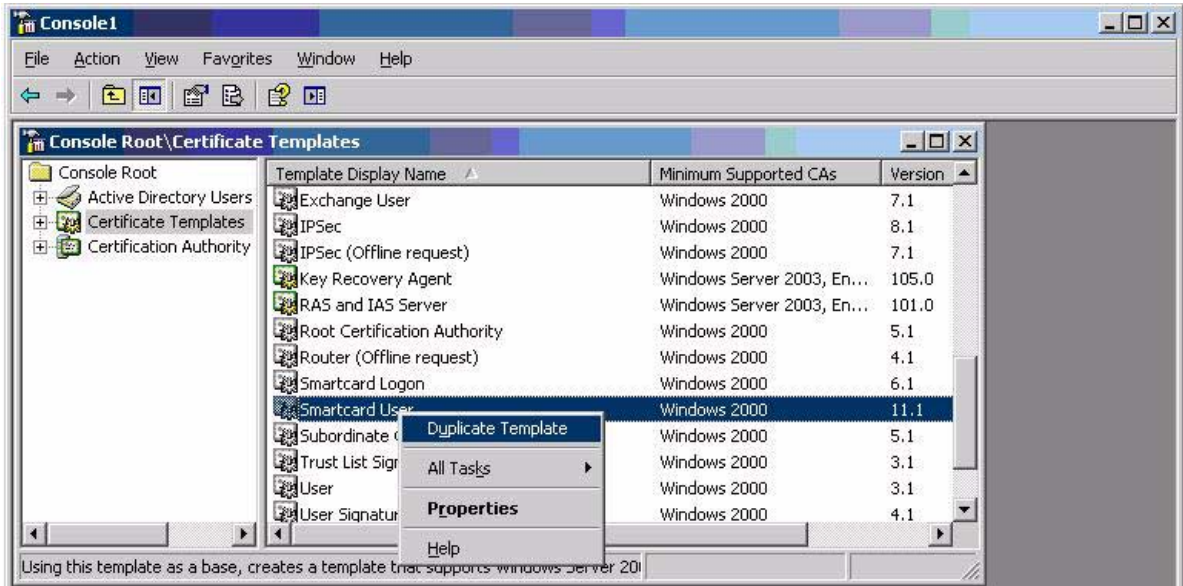
Configuring a Certificate Authority (CA) service

Configure a CA service. This white paper uses Microsoft Certificate Services to configure certificates. Refer to ["Installing Microsoft Certificate Services" on page 9](#) on installing certificate services.

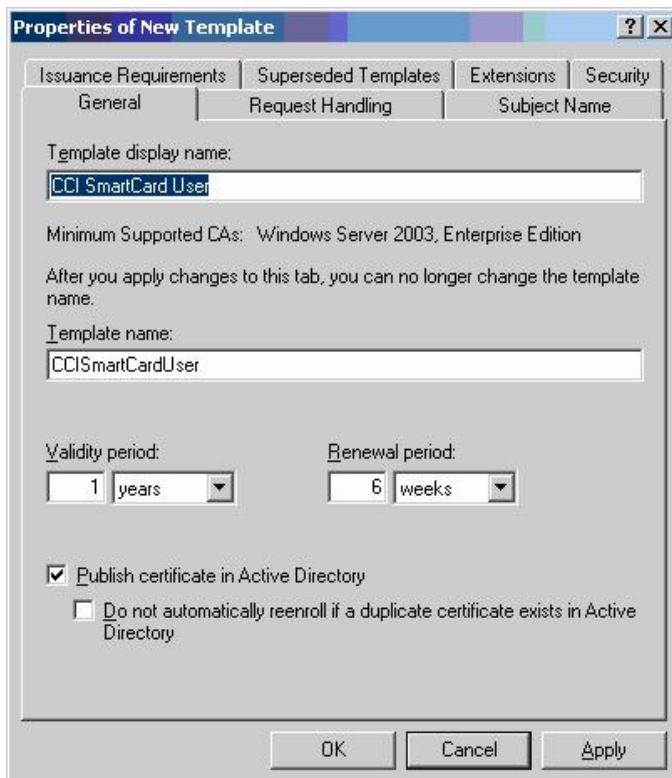
After you install the CA service, perform the following configuration steps:

1. Create a MMC with following snap-ins:
 - Active Directory Users and Computers
 - Certificate Authority
 - Certificate Templates
2. Click **Certificate Templates** and look for the Smartcard User certificate template in the right pane.

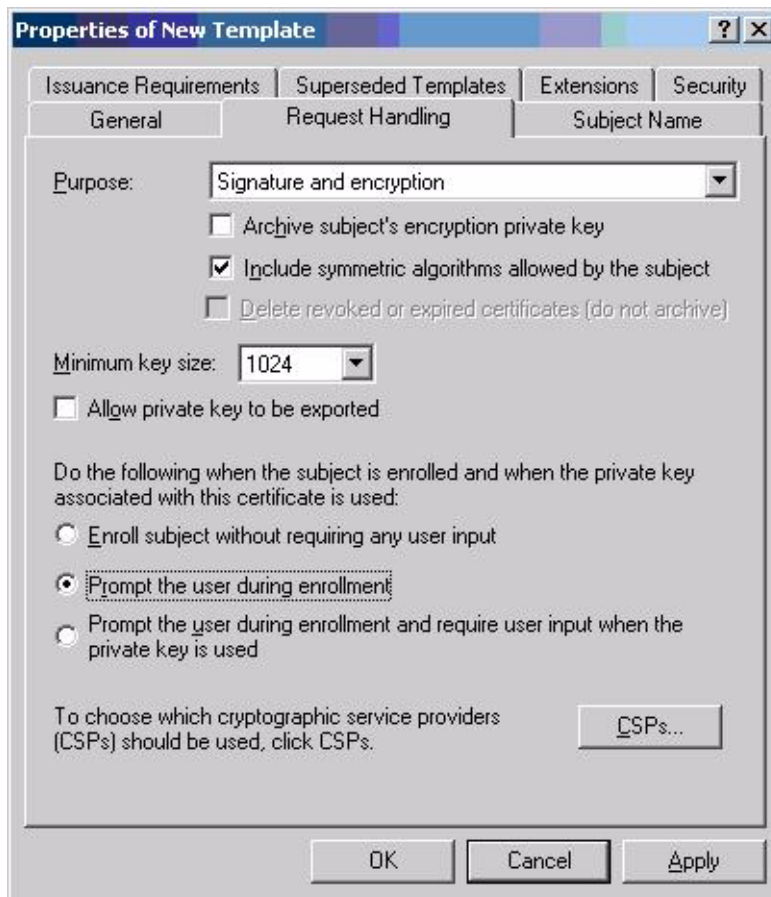
3. Create a duplicate template by right-clicking on the Smartcard Logon certificate template, and then selecting **Duplicate Template**.



4. Type a name for the new template in the **Template Display name** box. This example uses CCI Smartcard User

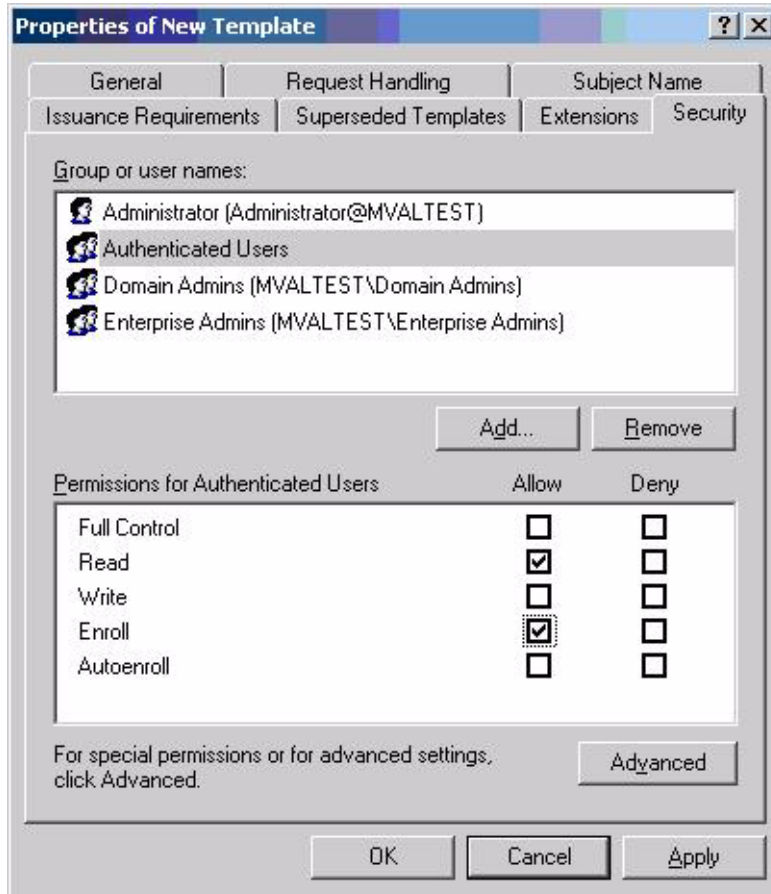


5. Click the **Request Handling** tab.



6. Select **1024** in the **Minimum key size** box.
7. Click the **CSPs** button.
8. Select **Requests can use any CSP available on the subject's computer.**
9. Click the **Security** tab.

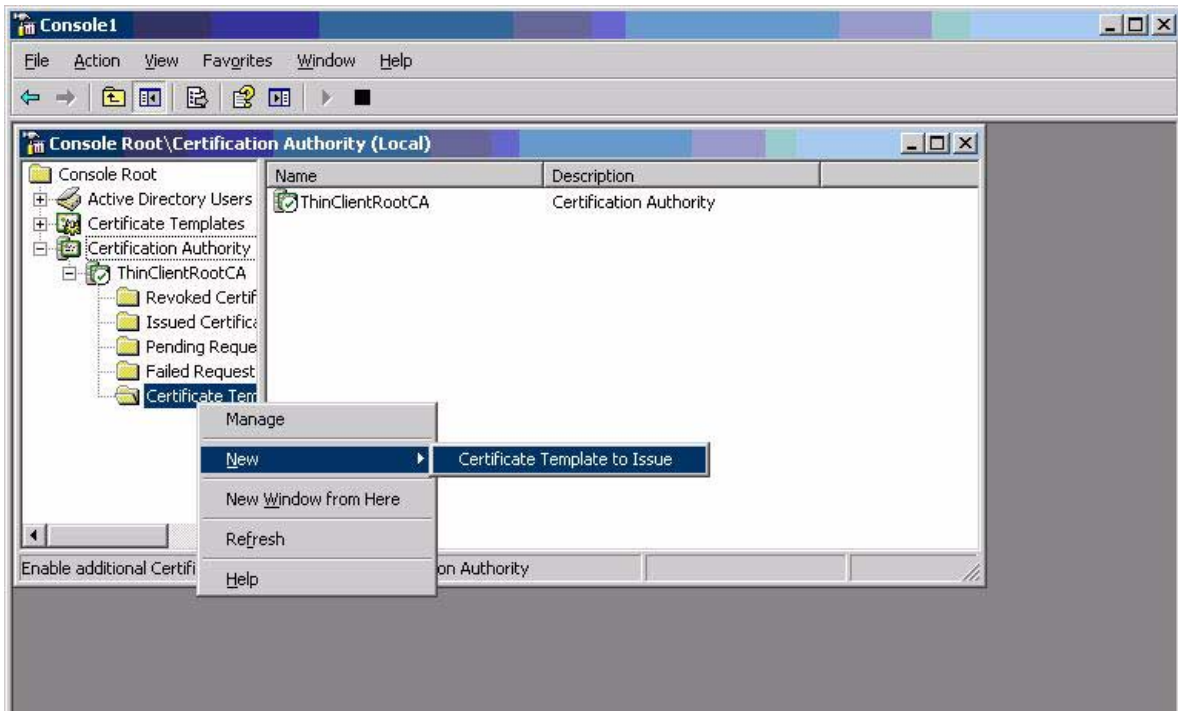
10. In the **Permissions for Authenticated Users** area, in the **Allow** column, select both **Read** and **Enroll**.



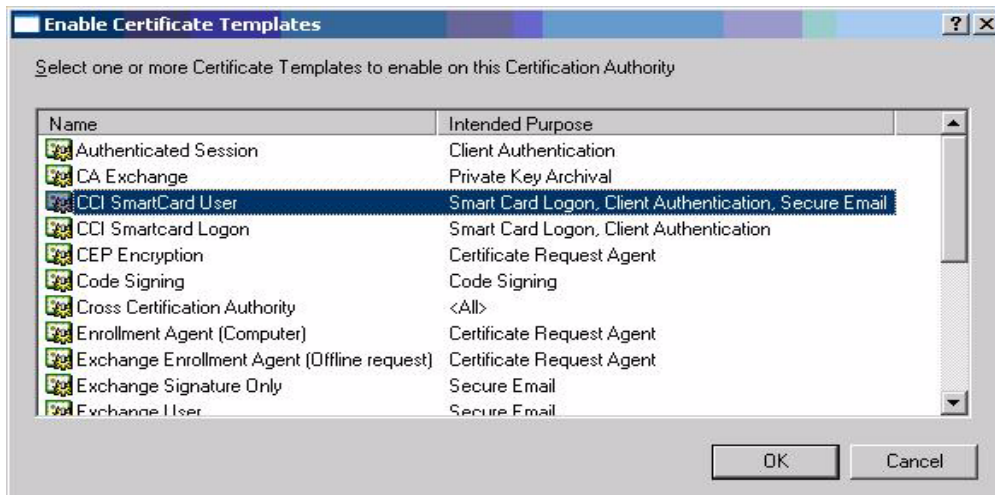
You have created the creation of the template.

11. Copy the *CCI SmartCard User* certificate template into the **Certificates Templates** folder under the certificate server.
- Expand the **Certificate Authority** object in the MMC you created in step 1.
 - Expand your CA name.
 - Right-click on the **Certificates Templates** folder under the CA server.

d. Select **New > Certificate Template to Issue**.

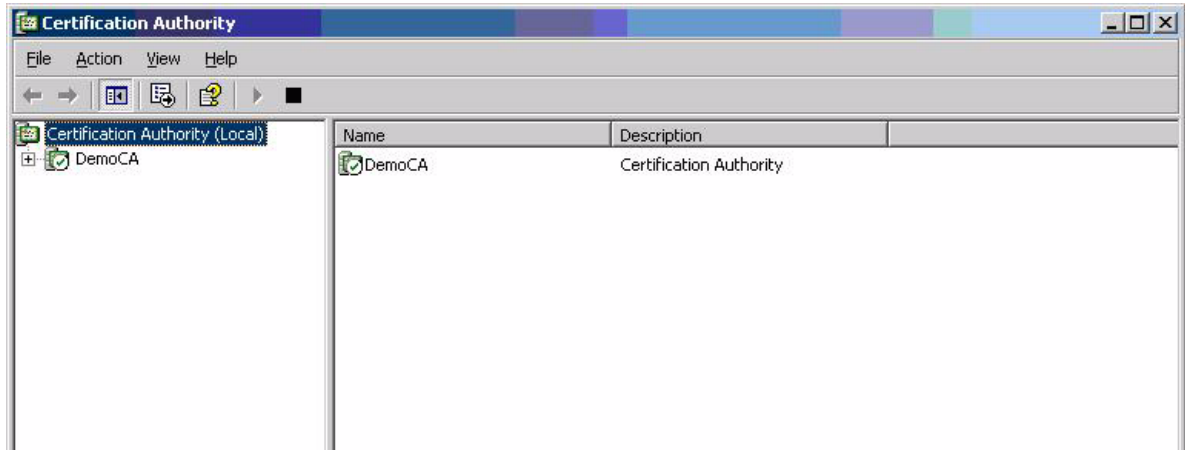


12. Select the template, and then click **OK** to import the template.

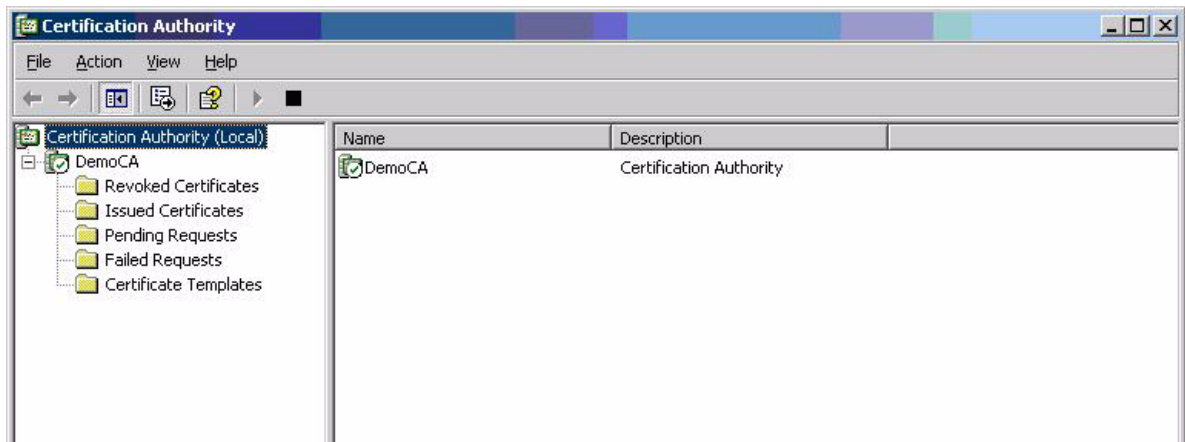


Configuring Microsoft Certificate Authority to Issue Smart Card User Certificate

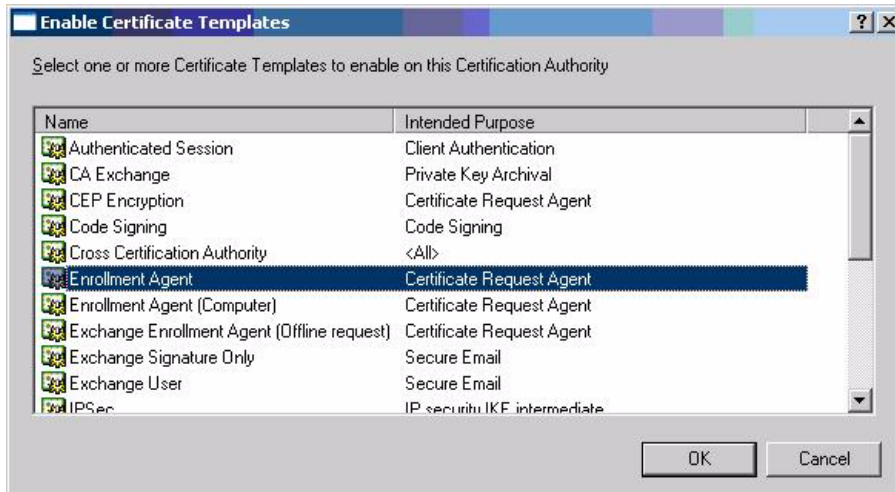
1. Click **Start > Administrative Tools > Certification Authority**.



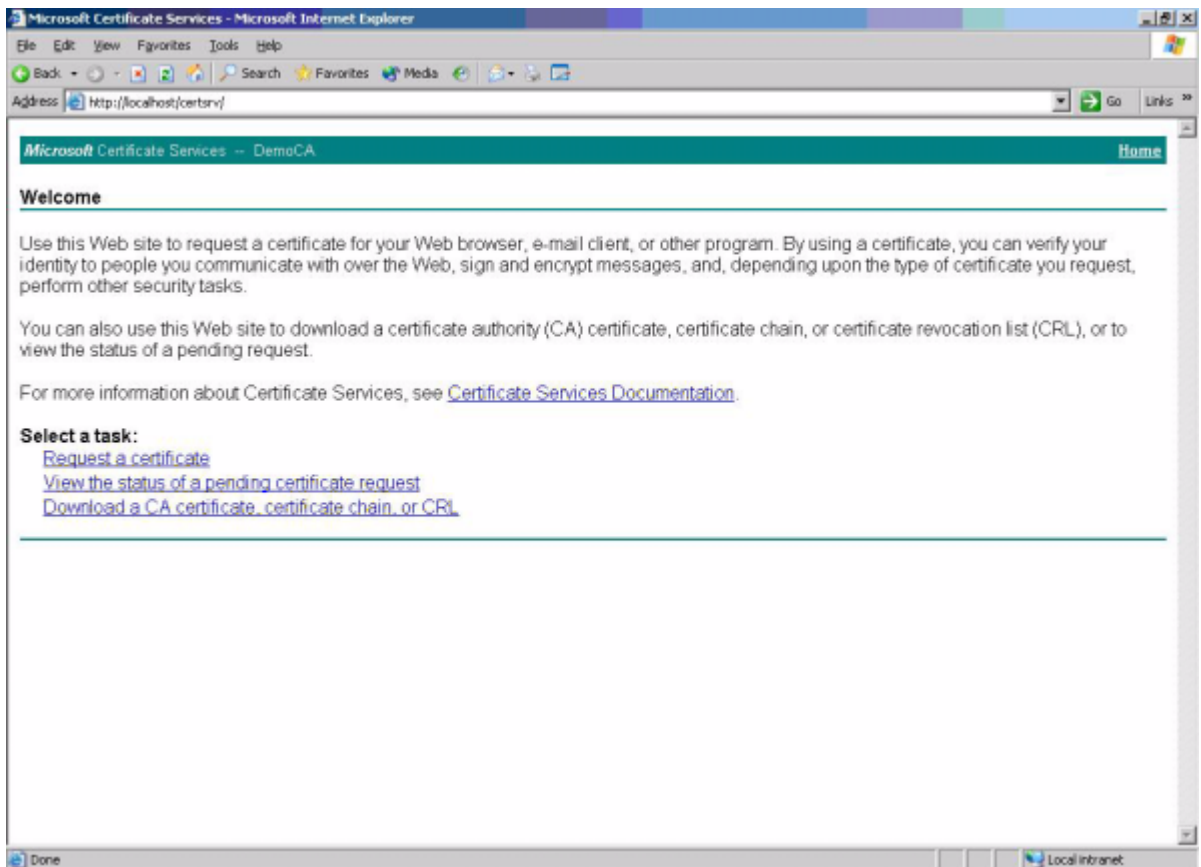
2. Expand the defined CA.



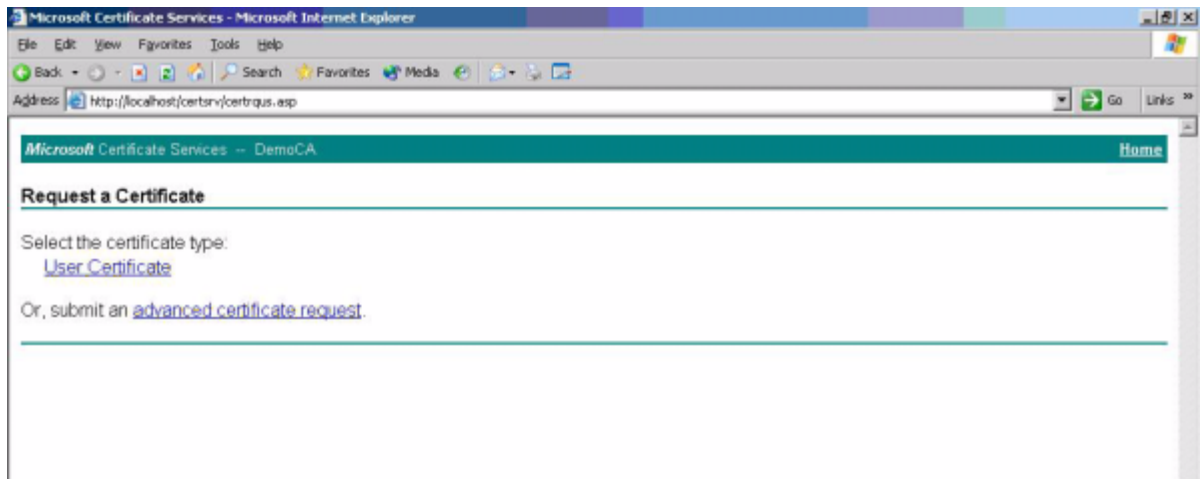
3. Right-click **Certificate Templates**, and then select **New**.
 - a. Select **Certificate Template to Issue**.
 - b. Select **Enrollment Agent**.
 - c. Select **OK** to add.



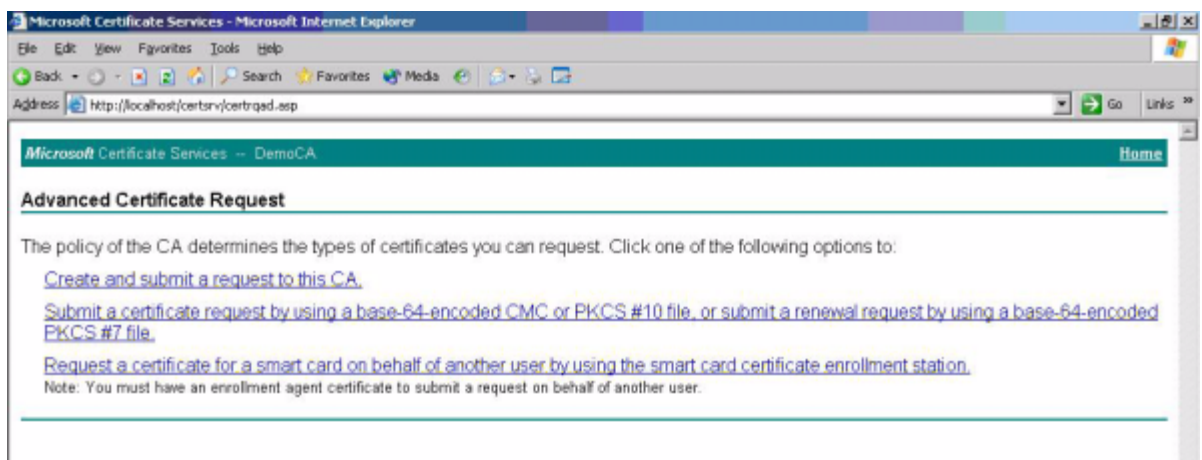
4. Launch Internet Explorer and browse to <http://localhost/certsrv>.
5. Under **Select a task**, select **Request a certificate**.



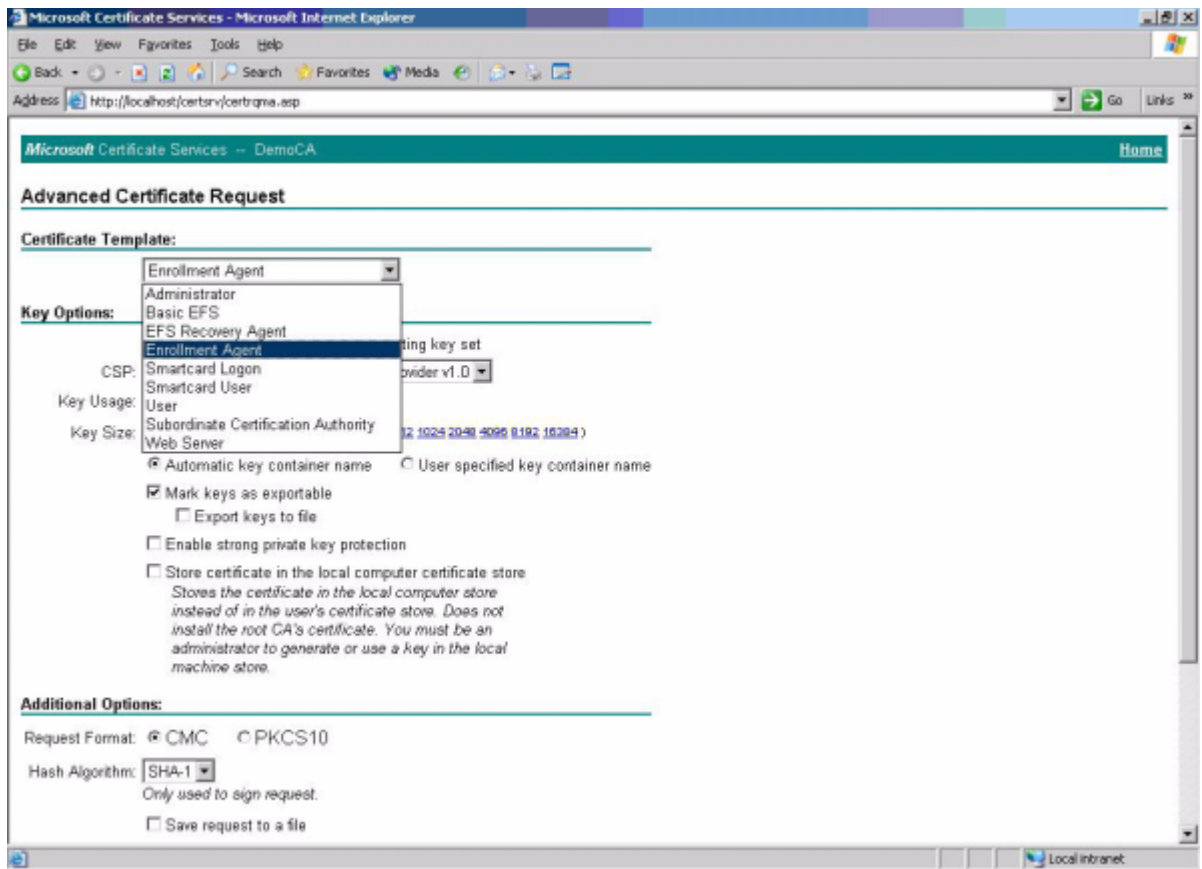
6. Select **advanced certificate request**.



7. Select **Create and submit request to this CA**.



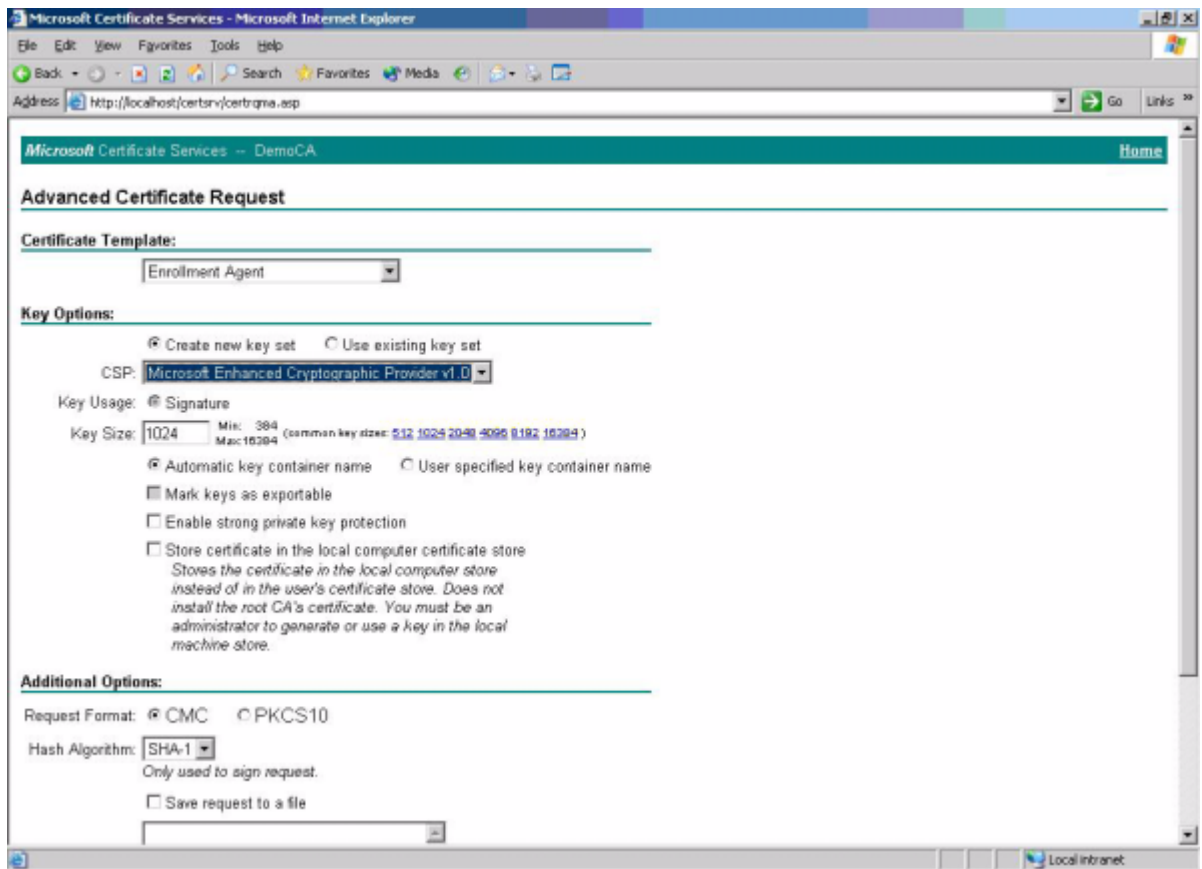
8. In the **Certificate Templates** box, select **Enrollment Agent**.



9. Verify Enrollment Agent Settings in the **Key Options** section as follows:

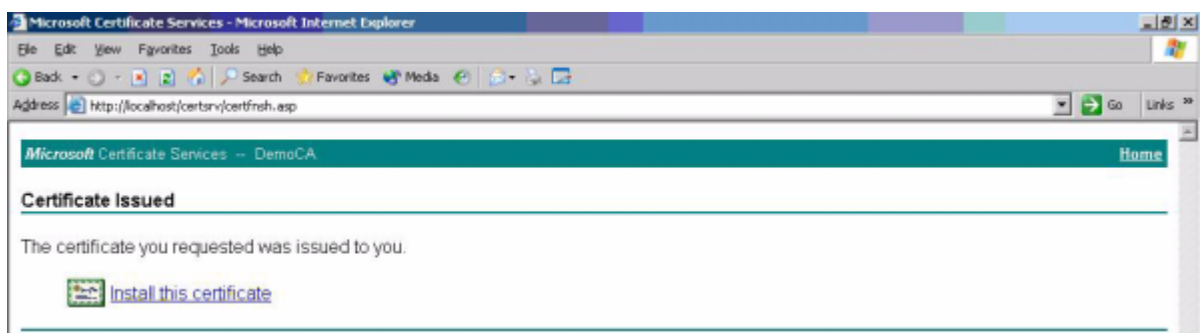
- **Create new key** is selected
- Microsoft Enhanced Cryptographic Provider v1.0
- Click **Submit**.

10. Accept default settings under **Additional Options**.



11. If a warning message displays about a potential scripting violation, press Yes to continue with the certificate request.

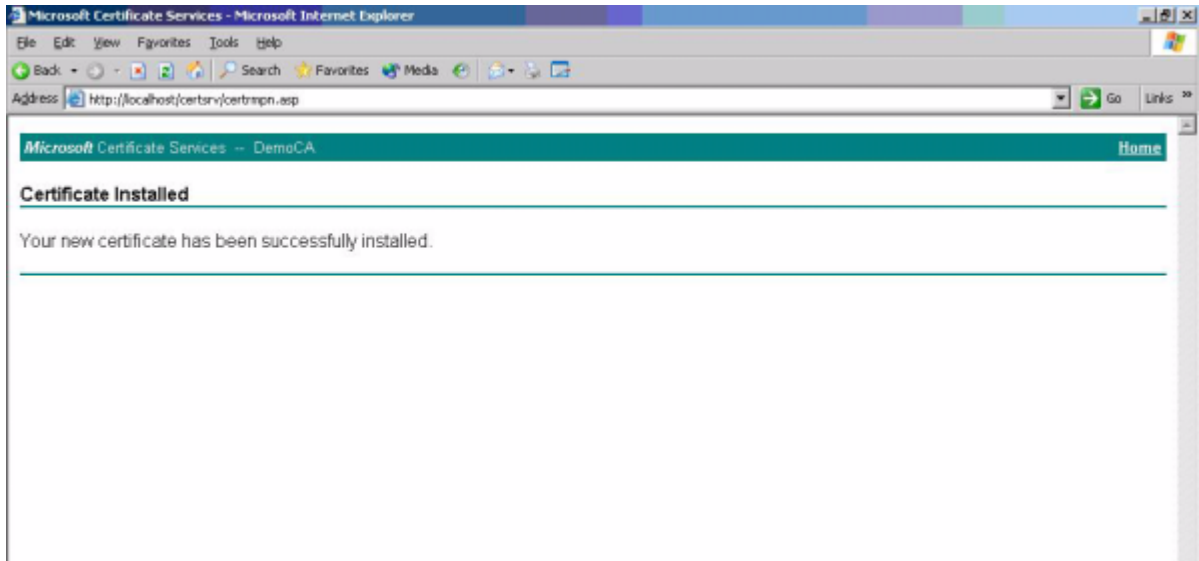
12. Install the Enrollment certificate requested.



13. Select **Yes** to Potential Scripting Violation.

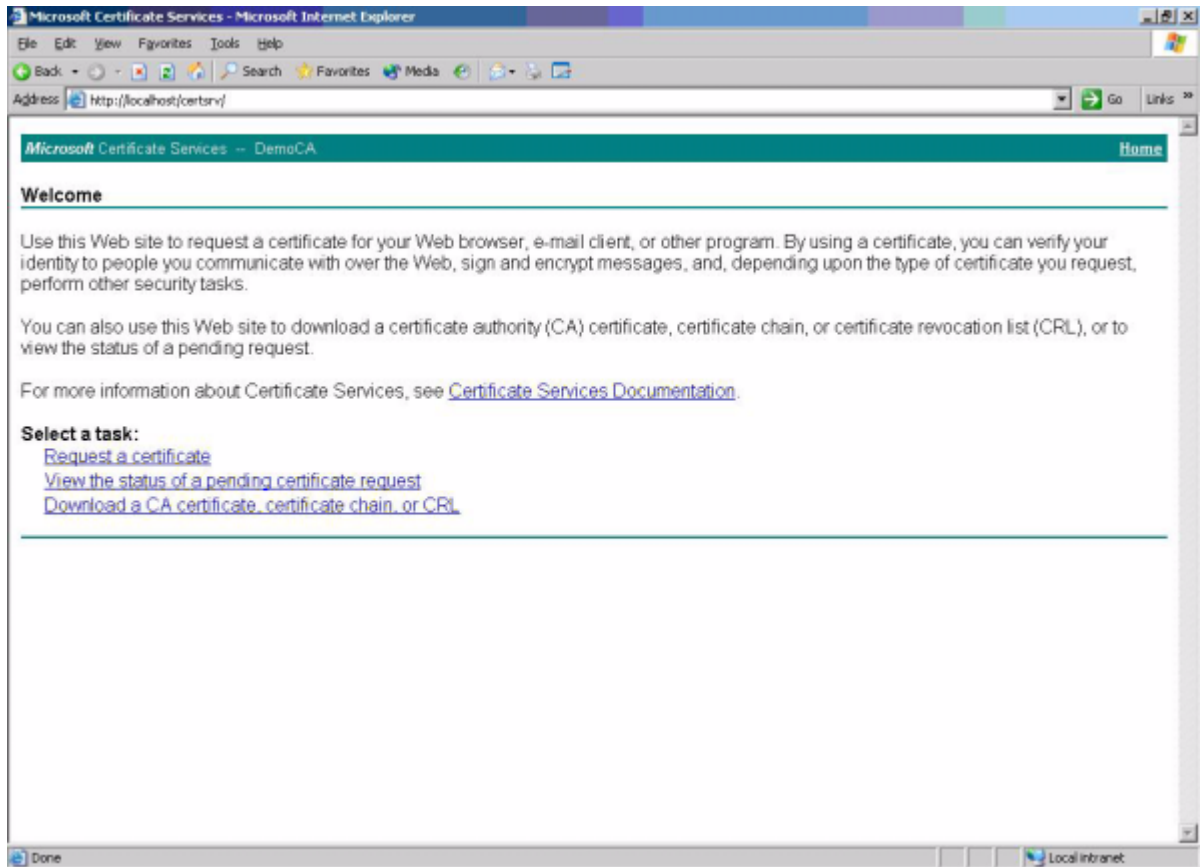


You have successfully generated and installed required Enrollment Certificate, as shown below.

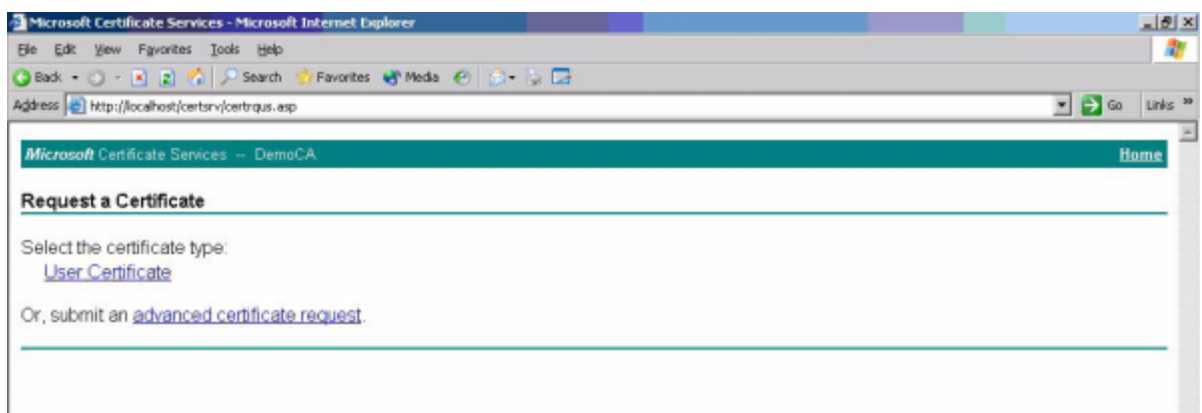


Manually issue Smart Card User Certificate

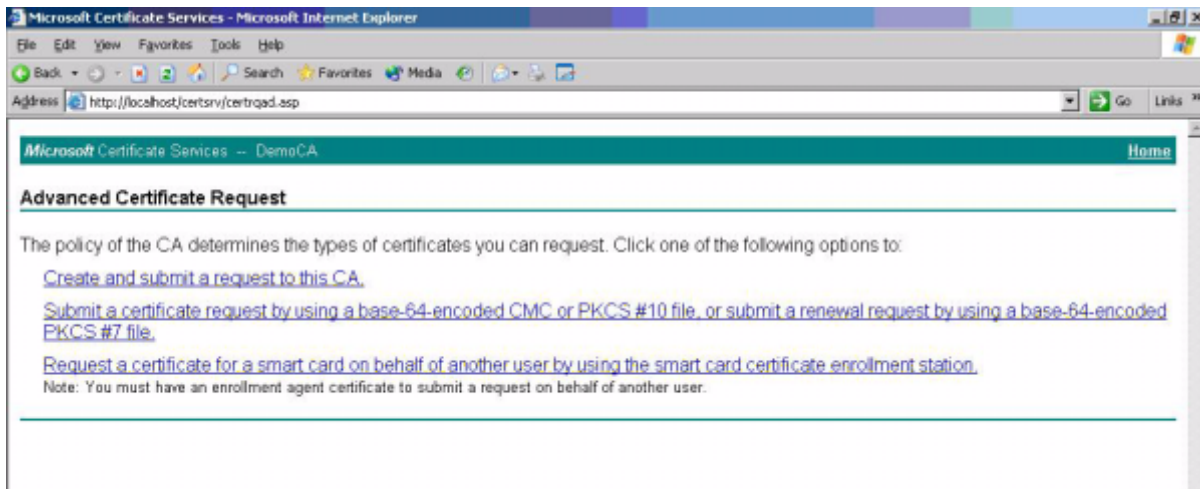
1. Launch Internet Explorer and browse to <http://localhost/certsrv>.
2. Select **Request a certificate**.



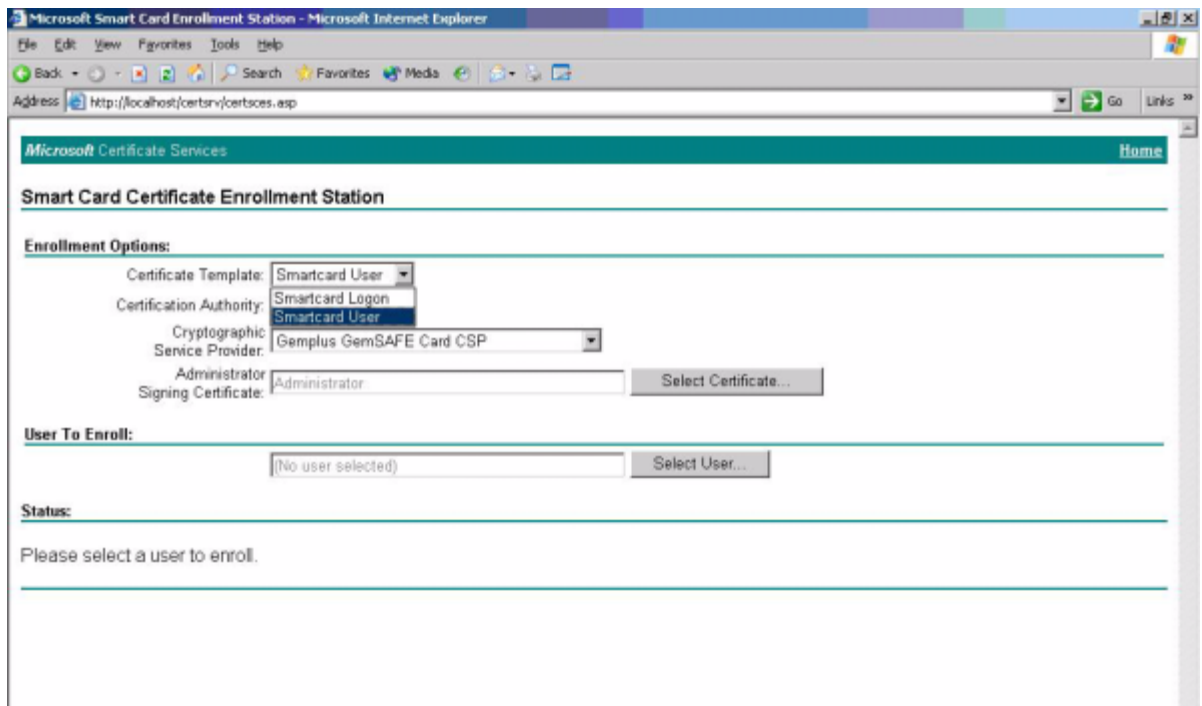
3. Select **advanced certificate request**.



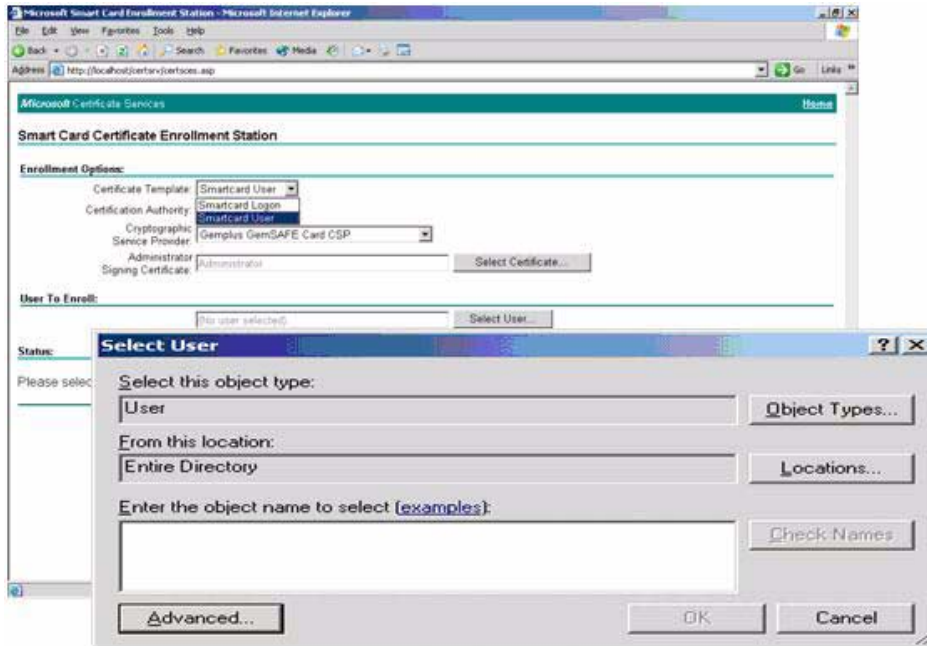
4. Select **Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.**



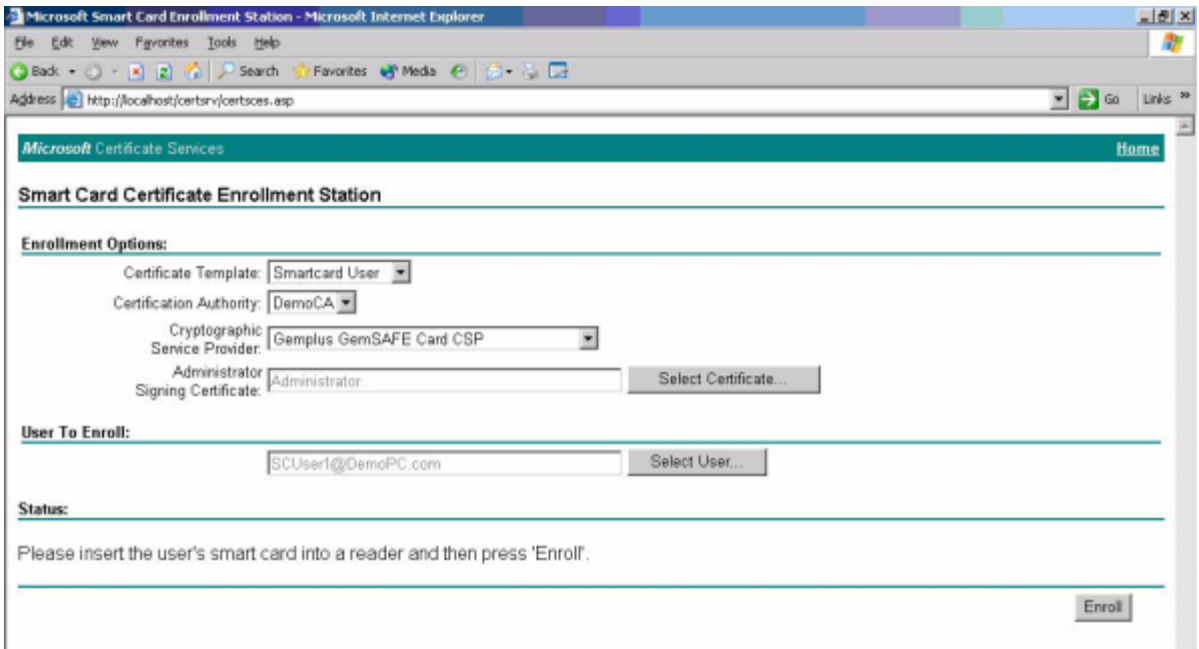
5. Select **Smartcard User** under **Enrollment Options.**



6. Define the user to enroll by clicking **Select User**.

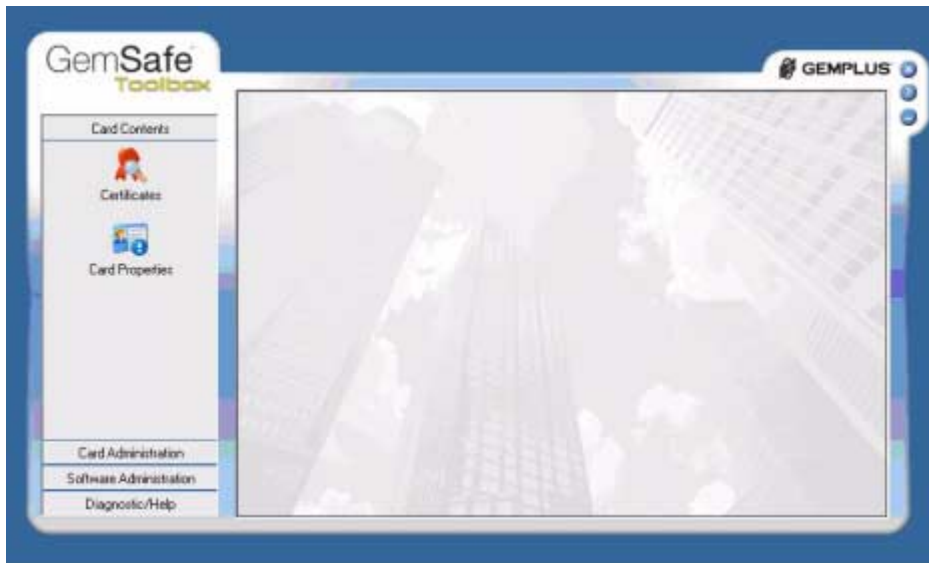


7. Insert **Smart Card into Reader**, and then select **Enroll**.

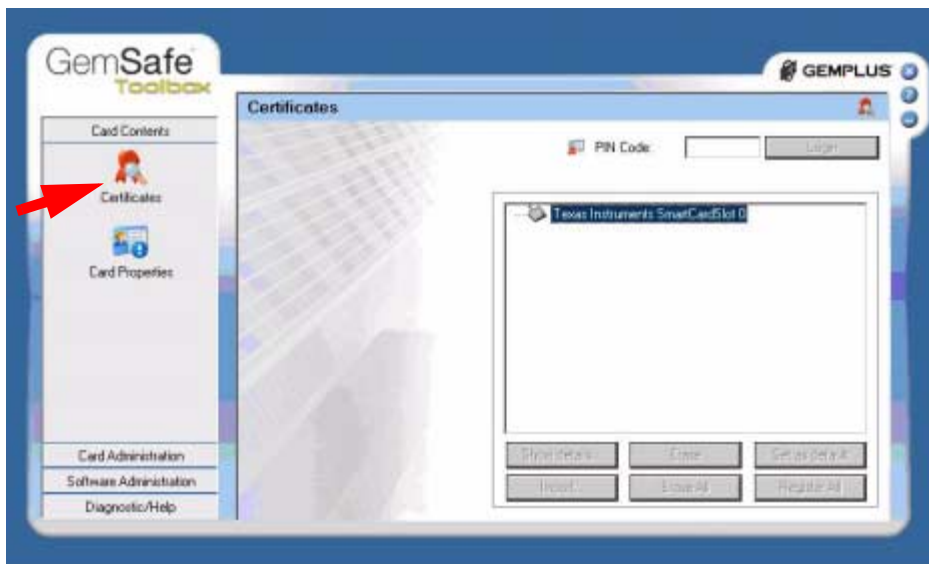


Testing the Smart Card

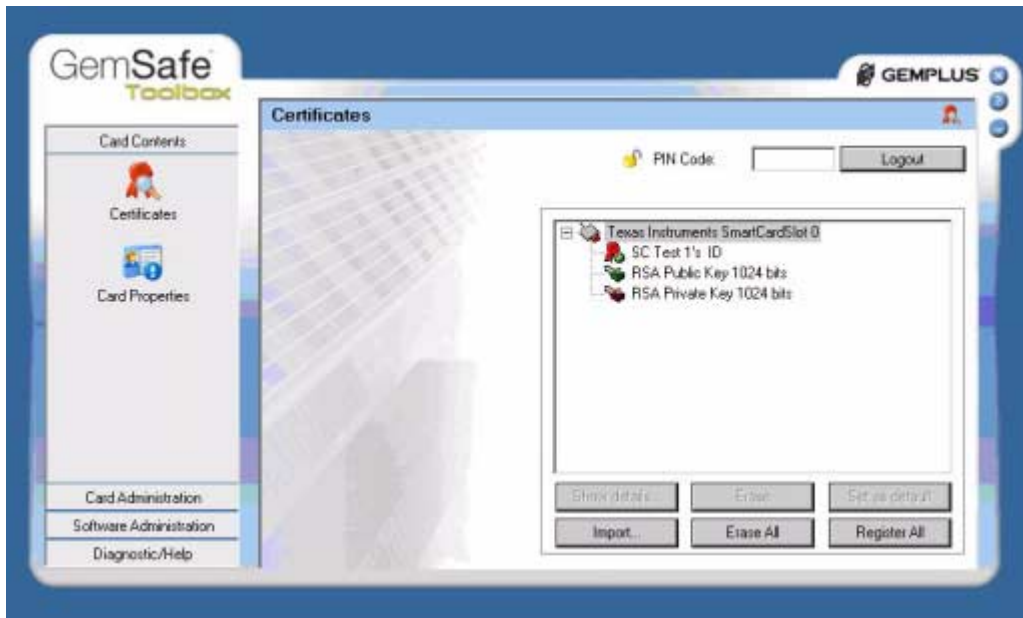
1. Launch the GemSafe Toolbox by selecting **Start > All Programs > Gemplus > GemSafe Toolbox.**



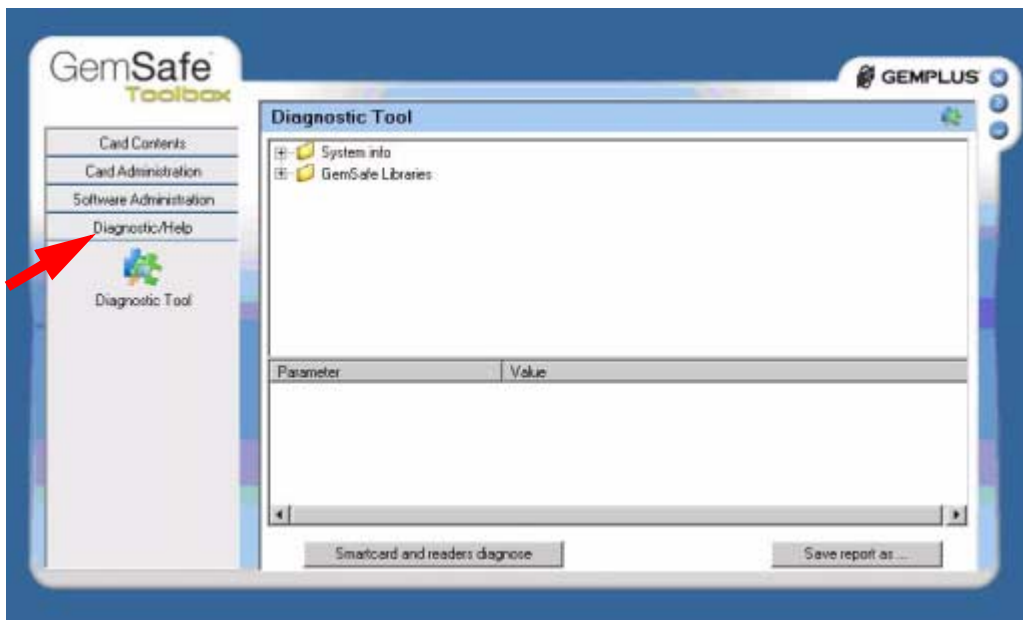
2. Select **Certificates.**



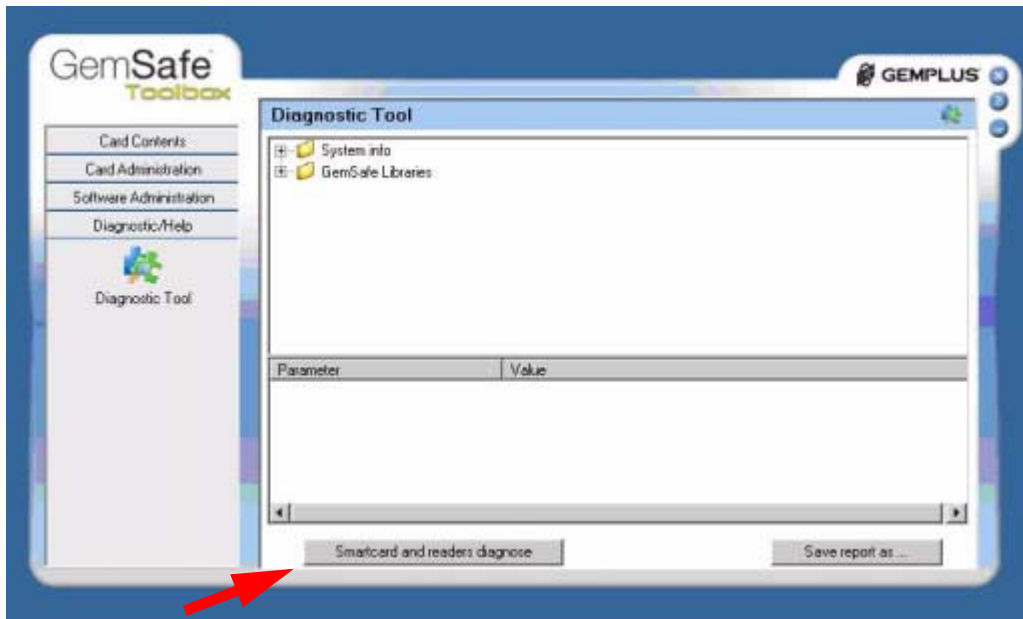
3. Insert the smart card and type the PIN. This displays the certificates that you manually issued to the card in **“Configuring Microsoft Certificate Authority to Issue Smart Card User Certificate”** on page 18.



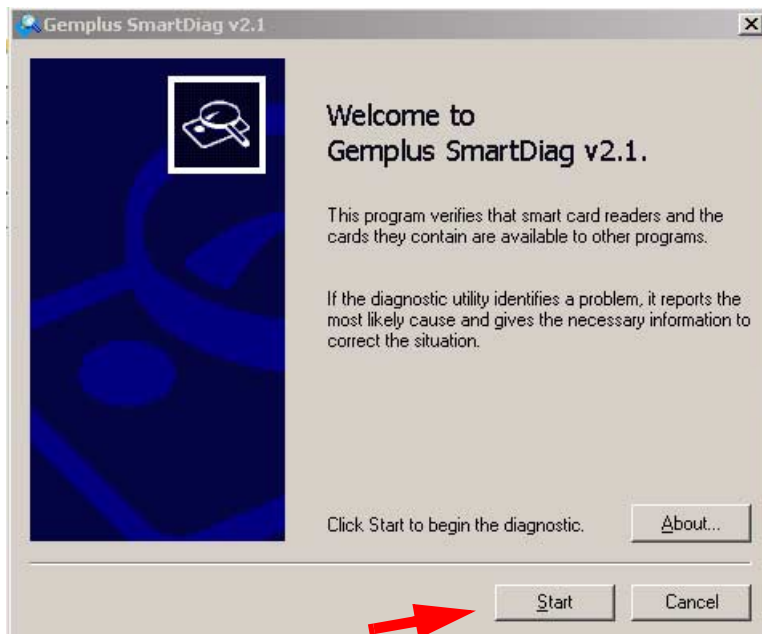
4. Select the **Diagnostic/Help** tab in the left frame.



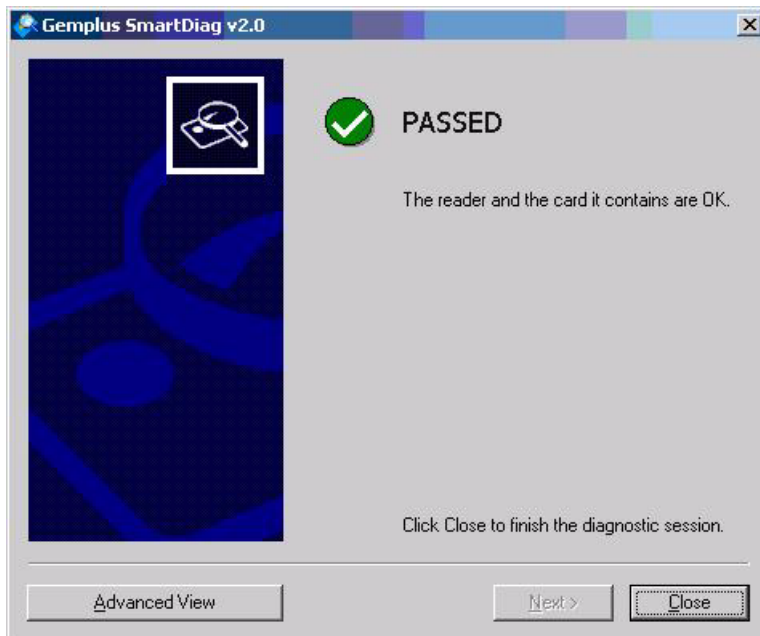
5. Select the **Smartcard and readers diagnose** button.



6. From the Smartcard Diagnostic Utility, select **Start**.



You should receive the following PASSED response.



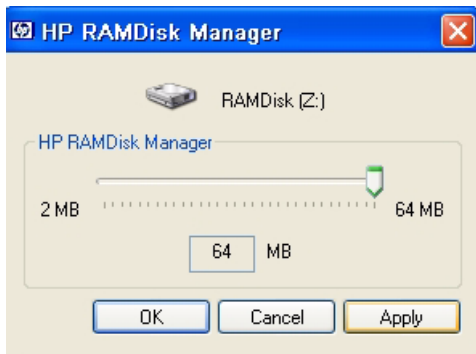
Creating Customized User Install Packages for Clients PCs (Optional)

The GemSafe user install package is not required for Domain logon smart card authentication with a pre-configured smart card that already contains a User certificate. Domain groups or user level policies for smart card login need to be managed and applied by the administrator. Administrators may wish to deploy a customized client GemSafe Toolbox to the client (as an example, for smart card properties or diagnostic capabilities).

NOTE: You must commit (EWF) the data to the volume or the data will be lost on the next reboot.

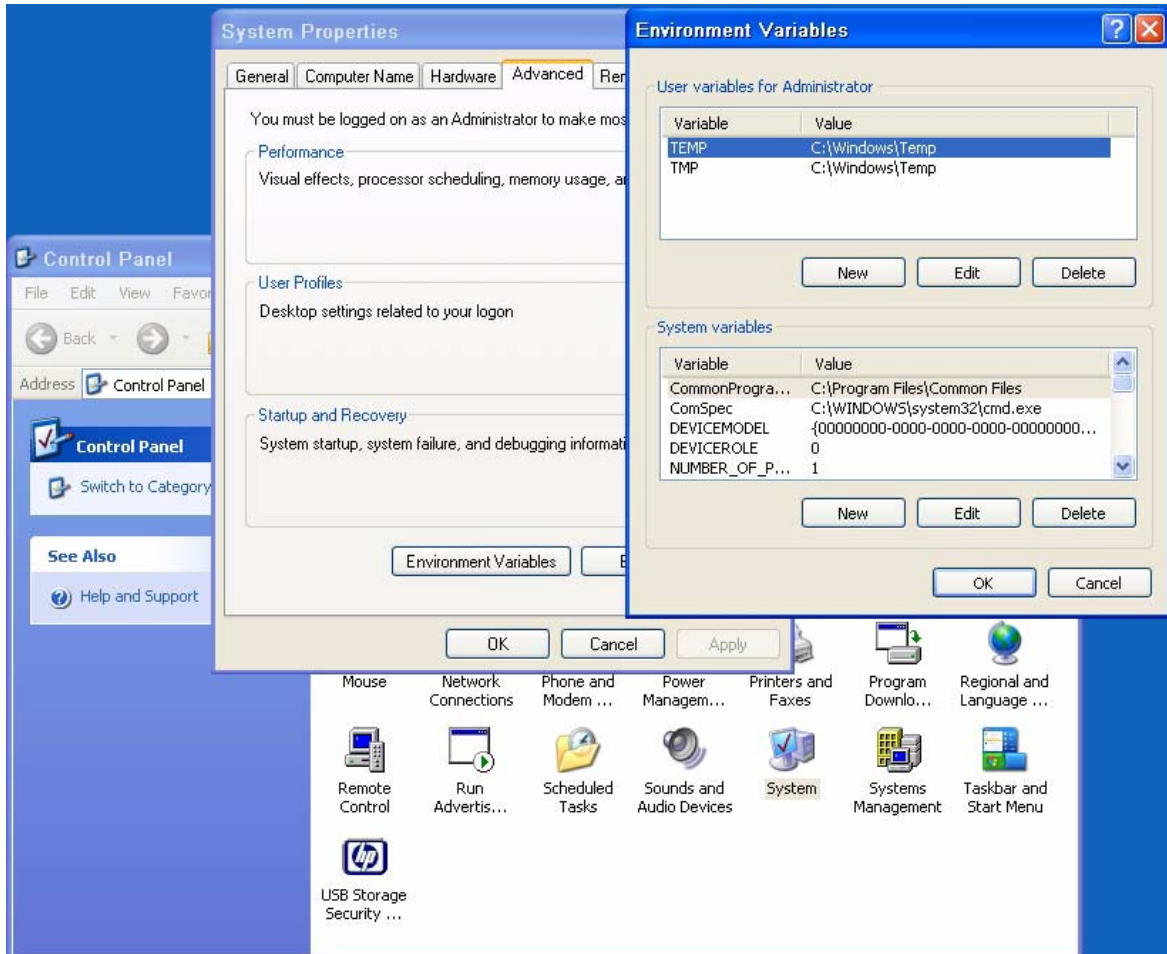
For thin client PC installation of the optional GemSafe ToolBox, modify the client's RAMDisk size from default settings up to 64-MB.

To change RAMDisk size, click **Start > Control Panel > HP RAMDisk Manager**.



For thin client PC installation of the optional GemSafe ToolBox, modify the thin client TEMP and TMP environmental variables to a location that can support the .msi user installation package size. The environmental variables can be changed back to default settings after installation package has been installed and write filter changes committed.

To change environmental variables, click **Start > Control Panel > System Properties > Advanced tab > Environmental Variables**.

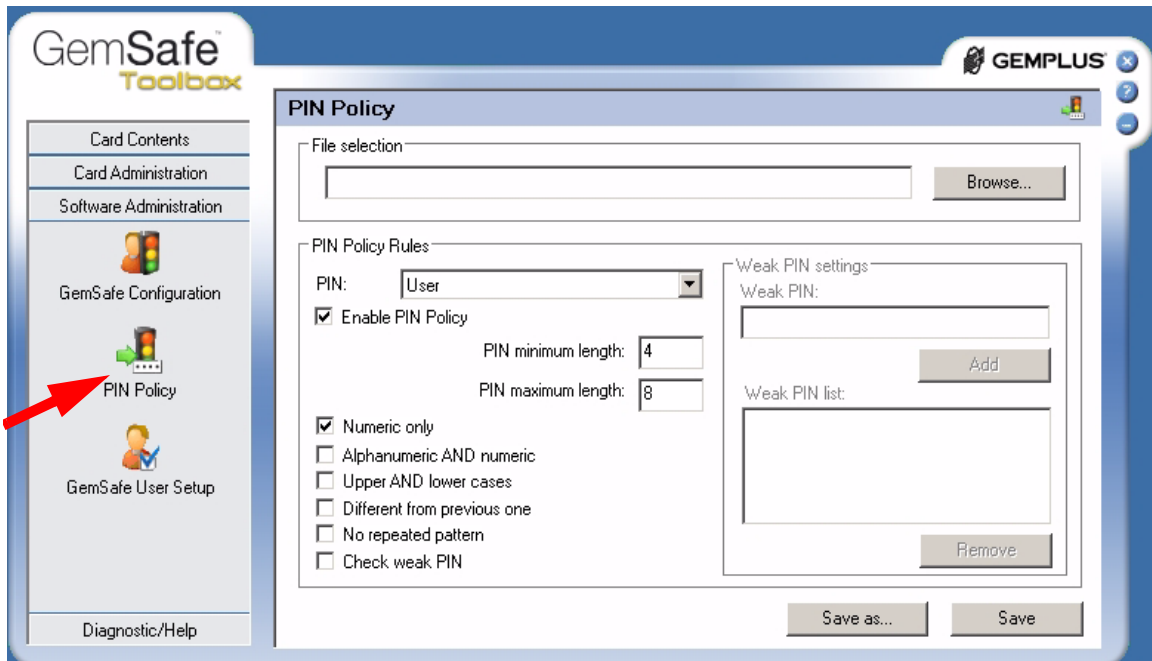


NOTE: HP deployment solutions such as Altiris client manager do not require Ram Disk size adjustments or modification of environmental variables.

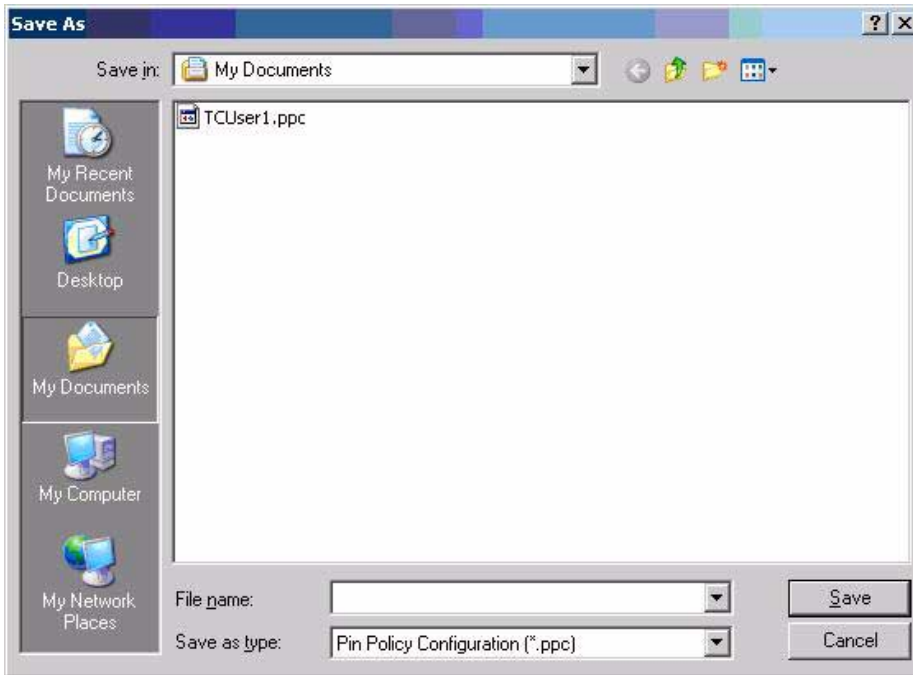
1. Launch the GemSafe Toolbox by selecting **Start > All Programs > Gemplus > GemSafe Toolbox**.



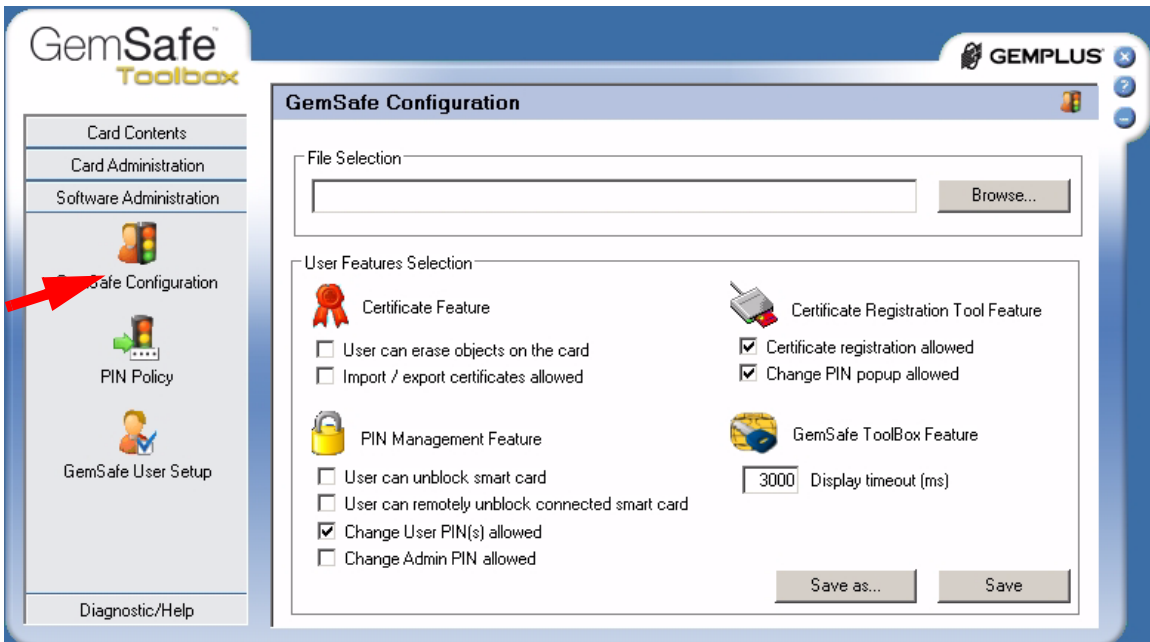
2. Select **Software Administration**.
3. Select **PIN Policy** in the left frame.



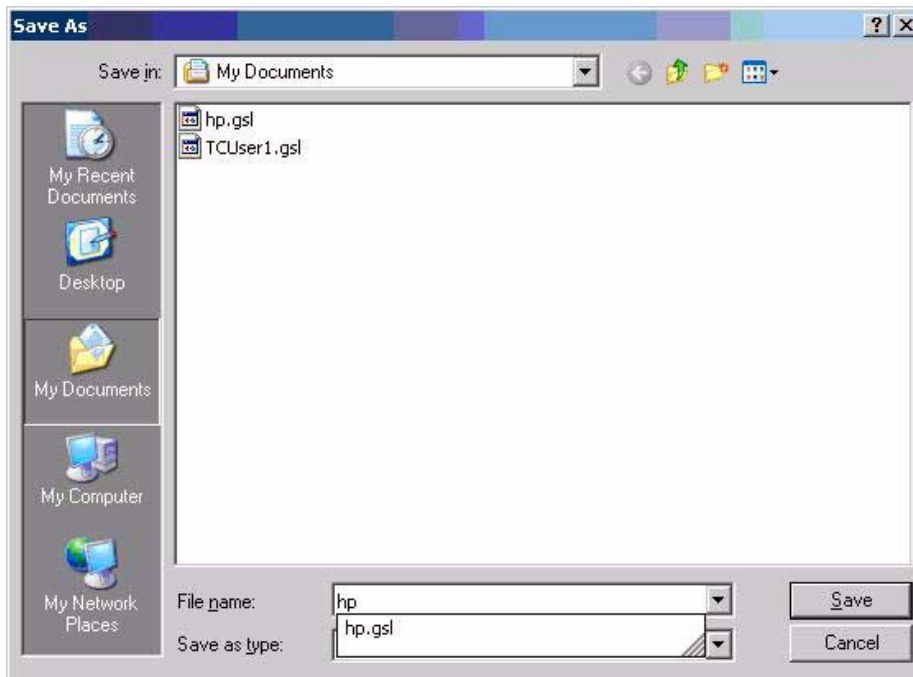
- To store PIN Policy settings, select **Save as**, and then type a file name.



- Select **GemSafe** in the left frame.
- Define what GemSafe Toolbox functionality will be provided to your users.



7. To store the user libraries configuration, select **Save as**, and then type the file name.

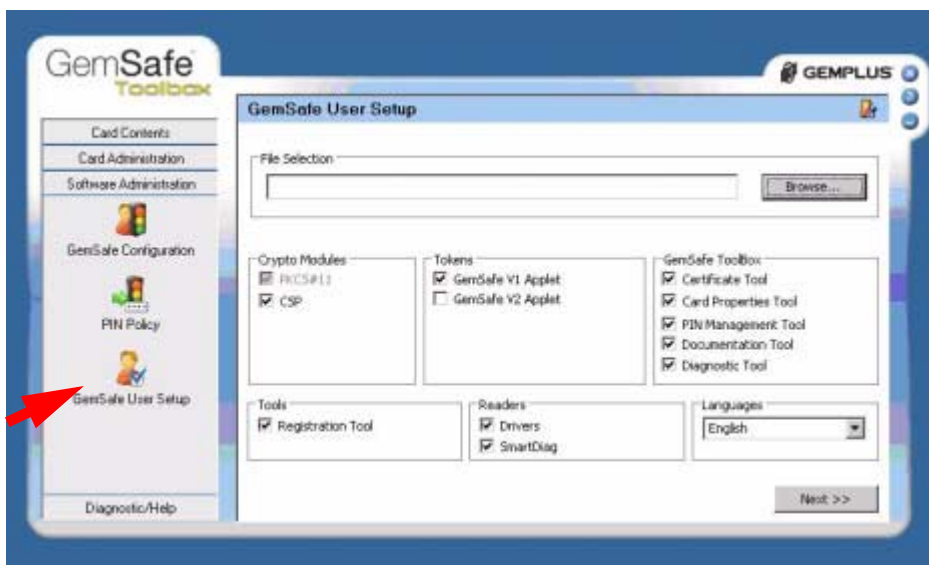


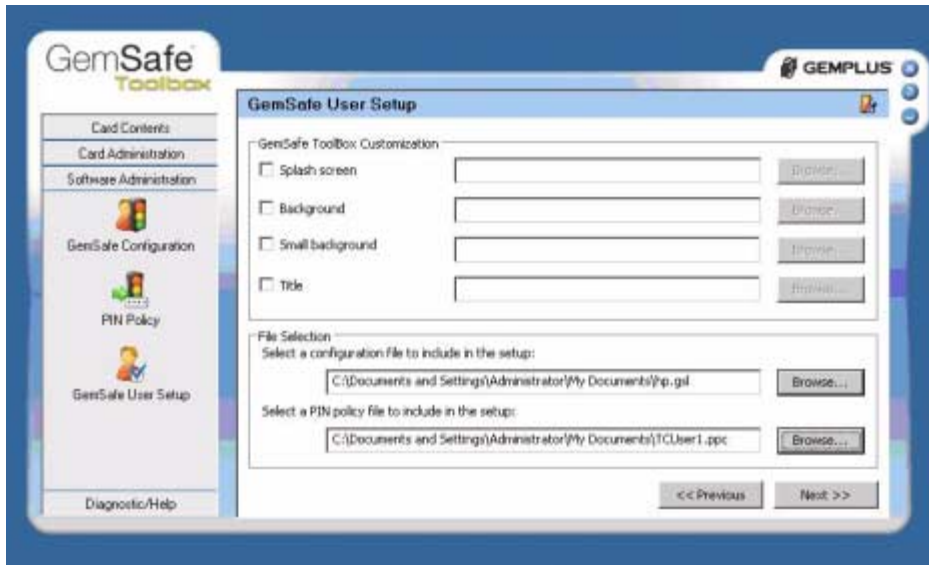
8. Select **Libraries User Setup** in the left frame, and then define Libraries User Setup.

NOTE: You must select CSP if you are operating in a Microsoft environment.

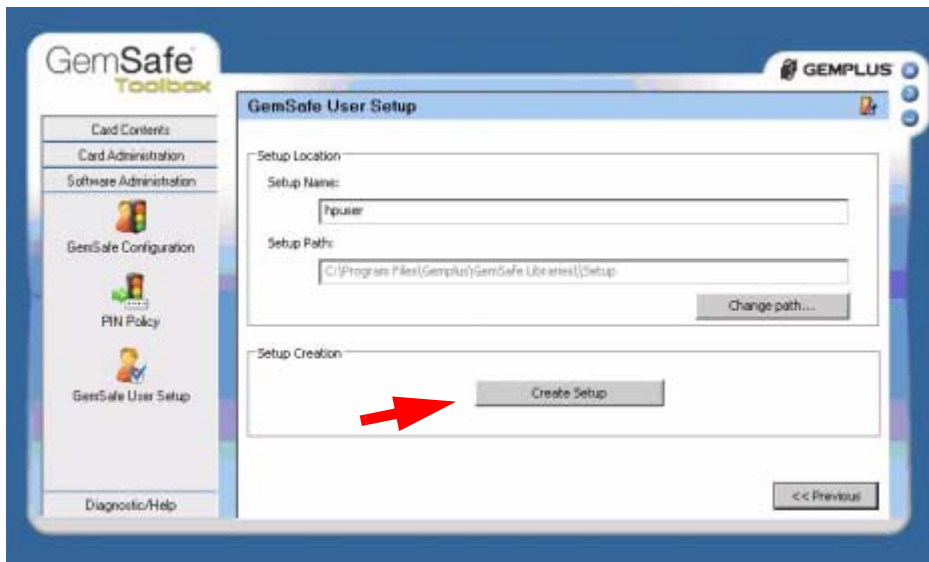
NOTE: If you planning on implementing on a Citrix or Terminal Services server.

- a. You must select the files you configured in step 4 - 7 within the **File Selection** section.
- b. Click **Next**.





- To provide a Setup Name for Libraries User Setup, select **Create Setup**. Be sure to note the setup path.



- Select **OK**. The new setup has been created.



The user package has been successfully created.

You can:

- Browse to the noted Path where package was created.
- Run Setup.exe on designated host.

Additional Information

Using a Smart Card For Windows Network Login

During windows logon, a normal Windows logon prompt should appear with a smart card reader icon on the left. After installing GemSafe Libraries users setups, restart the system. A normal Windows logon screen should appear with a smart card reader icon on the left. The system will recognize the smart card reader and will prompt you to insert your GemSafe smart card.

Upon the insertion of the GemSafe smart card into the smart card reader, you will be prompted to present a User PIN. By default, the User and Administrator PINs are '1234' unless the Administrator has previously set-up an alternate PIN. A User or Administrator is limited to three incorrect PIN entries before the PIN is blocked. Please check with your Administrator prior to submitting a PIN to ensure you have the proper one.

NOTE: If the User PIN is blocked, it can be unblocked if the Administrator has granted the User the right to unblock the PIN. If the user does not have this privilege, he or she should contact the Administrator to unblock the PIN. The Administrator can unblock the PIN by entering the Administrator PIN. However, if the Administrator enters three incorrect PINs in an effort to unblock a PIN, the card will no longer be usable.

Administration of the GemSafe Smart Card

Gemalto has designed the GemSafe ToolBox to manage GemSafe smart cards. The GemSafe ToolBox allows the User (based on privileges) or the Administrator to change and verify the PINs, view card and system information, and register certificates. For the Administrator, GemSafe ToolBox is used to create Users Setups by granting different access rights to users.

Working with GemSafe Libraries

Now that GemSafe Libraries is installed, please refer to the GemSafe Libraries Administration or User Guide to learn how to:

- Manage the smart cards and certificates used with GemSafe Libraries
- Use GemSafe Libraries to log on/off and lock/unlock your Windows 2000, XP workstation, Windows 2000 and 2003 Servers.
- Use a digital certificate to improve e-mail security and browse secure web sites.
- Use a certificate to sign Adobe Acrobat® or Microsoft Office XP or 2003 macros.



NOTE: Adobe Acrobat requires some additional configuration to enhance the security of PDF documents. Instructions on how to do this can be found within Adobe Acrobat Help under “Digitally Signing PDF Documents”.

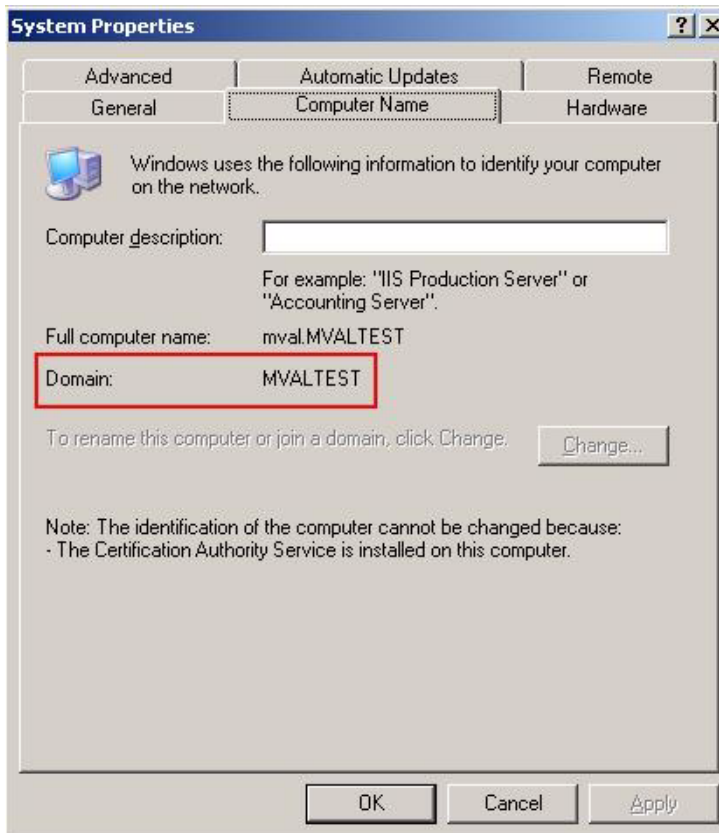
The Administration and User Guide also teaches security basics to help with the overall understanding of how GemSafe Libraries works to enhance your network security policy. The Guide also provides some Frequently Asked Questions (FAQs) to assist in troubleshooting problems that may occur.

Usage cases

Usage case 1: User authentication from blade PC to Active Directory Domain

The following steps provide instructions for performing a functional test of the CCI SmartCard Logon certificate (assumes Gemsafe libraries have been distributed to client PC's):

1. Ensure the CCI blade is connected to Active Directory Domain



2. "Log Off" or reboot the CCI blade.

3. Make sure a smart card is installed in the reader. The system requests the smart card PIN.



4. Type the PIN that you assigned. The user is logged into the Active Directory Server

Usage case 2: User authentication from client device to blade PC or Active Directory Server using RDP

The following steps provides instructions for performing a functional test of the CCI SmartCard Logon certificate:

1. Log out of the RDP session.
2. Open the Remote Desktop Communications window and initiate a connection to the blade.
3. Make sure a smart card is installed in the reader. The system requests the smart card PIN.



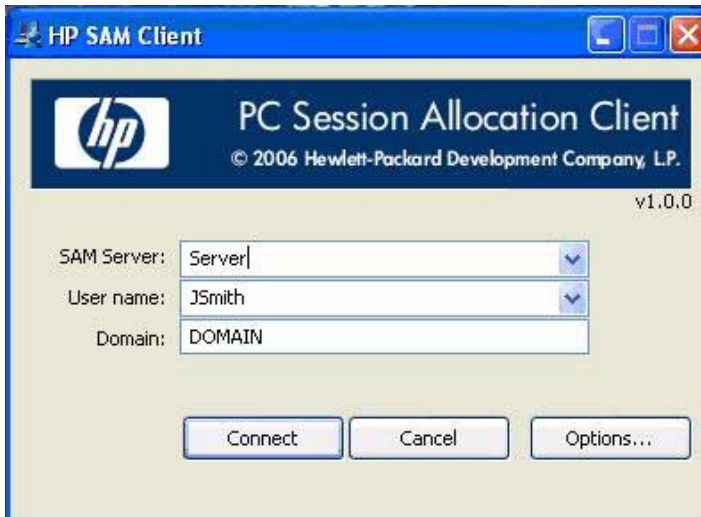
4. Type the PIN that you assigned. The user is logged into the blade

Usage case 3: User authentication from client device to blade PC or Active Directory Server using HPSAM client

The following steps provide instructions for performing a functional test of the CCI SmartCard Logon certificate:

1. Log out of the RDP session.

2. Open the HPSAM client window and initiate a connection to the blade PC or Active Directory Server.



3. Make sure a smart card is installed in the reader. The system requests the smart card PIN.

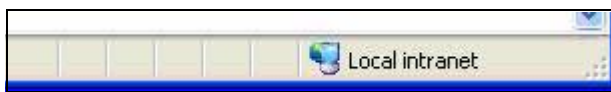


4. Type the PIN that you assigned. The user is logged into the blade PC or Active Directory Server.

Usage case 4: Accessing secure Web site

The following steps provide instructions for accessing a secure Web site using an Gemalto smart card through a blade PC or Active Directory Server. Installing and configuring a secure Web site is beyond the scope of this white paper; therefore, the white paper assumes the secure Web site is already functional and accessible from the blade PC or Active Directory Server. The white paper also assumes that you can use the certificate installed on the smart card to access this secure Web site.

1. Log in to a blade PC or Active Directory Server using a smart card, as demonstrated in usage case 1.
2. Use Internet Explorer to connect to a Web site to make sure the system is functioning properly. Connect to a Web page on the same server as the secure Web site.
3. Confirm that the lower right corner of the Internet Explorer window does not display a lock icon.



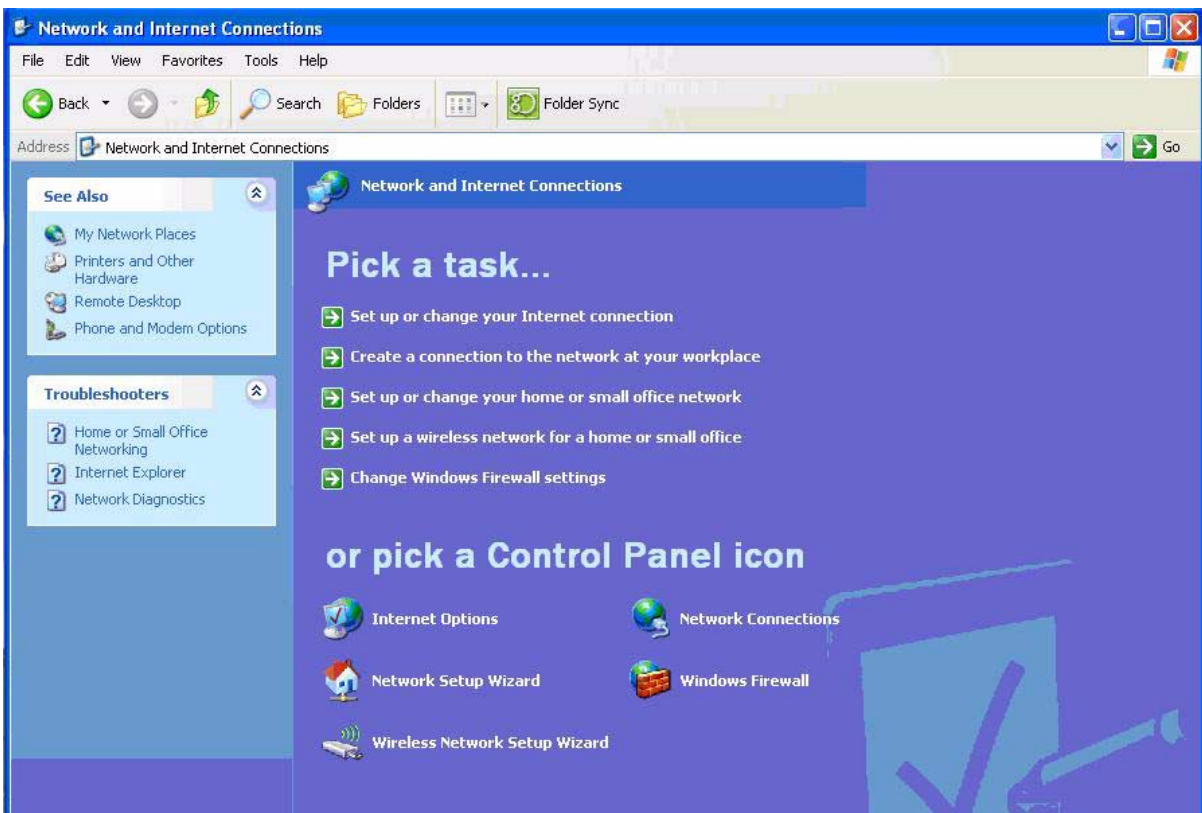
4. In Internet Explorer, type the address of a secure Web site.
5. If the system displays security alert messages, click **OK**.
The LED on the card reader indicates when the Web site is accessing the smart card to verify whether the certificate is approved for the site.
6. After the secure Web site displays, a lock icon in the lower right corner of Internet Explorer confirms that you are connected to a secure Web site.



Usage case 5: User authentication using VPN through firewall to blade PC or Active Directory Server

Instructions for installing and configuring a VPN tunnel with a firewall is beyond the scope of this white paper; therefore, the white paper assumes the VPN tunnel and firewall are already installed and functional. The white paper also assumes that you have a broadband Internet connection and that Gemalto smart card middleware is installed on the client.

1. In the Control Panel on the client computer, open **Network and Internet Connections**.
2. Select the **Create a connection to the network at your workplace** task.



3. In the New Connection Wizard, select **Virtual Private Network connection**.

4. In the **Company Name** box, type the name for the VPN connection (for example, *work*), and then click **Next**.
5. Select **Do not dial the initial connection**, and then click **Next**.
6. In the text box, type the host name or IP address of the VPN tunnel, and then click **Next**.
7. Select **Use my smart card**, and then click **Next**.
8. Select **Add a shortcut for this connection to my desktop**, and then click **Finish**.



Depending upon the configuration of the VPN tunnel, you may have to change the configuration of the VPN connection.

To change the configuration of the VPN window:

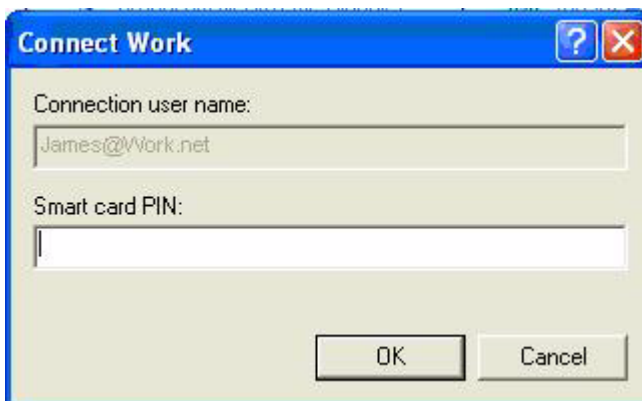
1. In Control Panel, open **Network and Internet Connections > Network Connections**.

2. Right-click on the **VPN connection** icon and select **Properties**.



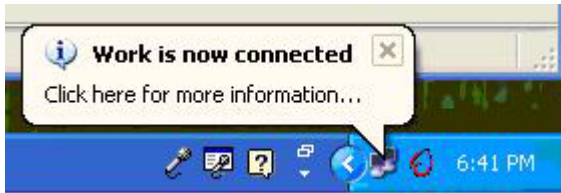
You can initiate the VPN connection after setting it up, as follows:

1. Start the VPN connection.
2. In **Smart card PIN**, type the PIN, and then click **OK**.



While establishing the VPN connection, the system displays *Verifying* username and password and *Authenticated*.

After the connection is established, the network connection icon displays in the system tray.

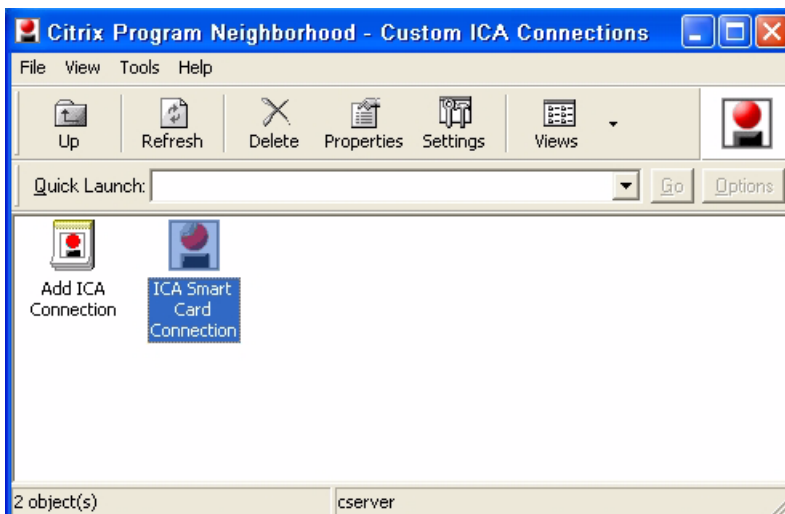


Usage case 6: User authentication from client device using Citrix server

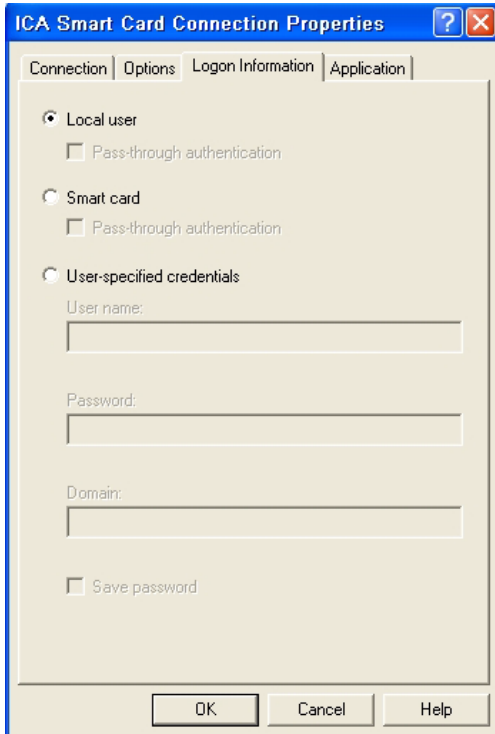
1. Click the **Citrix Program Neighborhood** desktop shortcut.



2. Click **Add ICA Connection** to set up a new client connection or to use a pre-existing Citrix connection.



3. Select properties for the ICA connection, click the **Logon Information** tab, select **Smart card**, and then click **OK**.



4. Double-click the shortcut to connect to the Citrix server.
5. During logon to the server, the smart card login prompt appears for authorization.



Service and Support

If you would like additional information about GemSafe Libraries 4.2.i, you can visit:

http://www.gemplus.com/products/gemsafe_libraries.

For product information, local sales offices, please visit **<http://www.gemalto.com>**, or send an email to: **HP@gemalto.com**.

Phone: (888)-343-5773.

© 2007 Hewlett-Packard Development Company, L.P. The information in this document is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft, MS-DOS, Windows, and Windows NT are trademarks of Microsoft Corporation in the U.S. and other countries.
450758-001, 4/2007

