Implementing ActivIdentity Smart Cards for Use with HP Compaq t5720 Thin Clients and HP Blade PCs

Introduction

Smart cards can strengthen user authentication in a corporate network by offering strong, 2-factor authentication to offset weak passwords or cumbersome authentication policies requiring frequent password changes. This paper provides instructions for configuring a smart card with your HP Compaq t5720 Thin Clients and HP blade PCs. This white paper is not intended as a comprehensive overview of ActivCard smart card technology and does not address detailed setup of network infrastructure settings such as DHCP, DNS, Active Directory, IIS or the HP Session Allocation Manager (SAM) or other Windows load balancing concerns.

This white paper assumes working knowledge for configuration of Thin Client Enhanced Write Filter (EWF) and acknowledged RDP enablement settings at both server and client.

Prerequisites

1. ActivClient software for HP ProtectTools Java Card, 3rd party DoD Common Access Card, as well as the target operating system (Windows) require different ActivIdentity libraries. To use this paper, you must have the proper software installed for your environmental needs. Please consult with ActivIdentity to ensure you purchase the appropriate software for your card provisioning and operating system support.
   - ActivClient for PKI Only 6.0
   - ActivClient for CAC - PKI Only 6.0
2. User has local administrative rights.
3. Windows 2000 SP3 or higher.
4. Microsoft Outlook 2000 SP3, Outlook 2002 SP3, Outlook 2003, without Service Pack or with SP1 or SP2 supported.
5. HP ProtectTools Java Card: 405674-001. You can acquire bulk purchase of 10 cards through the HP Parts Store at: **http://h20141.www2.hp.com/hpparts/Search_Results.asp?cc=US&SearchInc=PartNumber&lang=EN&jumpid=hpr_R1002_USEN&SearchCriteria=405674-001**
6. Smart card reader architecture: PC/SC
7. Microsoft Internet Explorer 5.5 SP2, Internet Explorer 6 (without SP, with SP1 or SP2), Internet Explorer 7 RC1, Netscape 4.76 and 7.1, Mozilla 1.7.3, Firefox 1.5.0.4.
8. Citrix Server version support:
   - MetaFrame XP Presentation Server FR3 SP4 on Windows 2000 (with Citrix hot fix XE104W2K002, available on Citrix Knowledge Base - Document ID CTX105789)
   - Citrix Metaframe XP FR3 SP4 (on W2K and W2K3), and on Windows 2003 Server (with Citrix hot fix XE104W2K3003, available on Citrix Knowledge Base - Document ID CTX105791).
   - Citrix Presentation Server 4 with Hotfix Rollup Pack PSE400W2K3R01 for Citrix Presentation Server 4.0.
   - Citrix Access Essentials 1.0 for Windows Server 2003.

- Citrix Presentation Server 4 with Hotfix Rollup Pack PSE400W2KR01 for Citrix Presentation Server 4.0 for Windows 2000 Server.
- Fat clients:

  - Client (Windows 2000/XP): MetaFrame Presentation Server Client Packager 8.1, Program Neighborhood Classic component.

  - Citrix Presentation Server Client Packager - Version 9.200

  - Program Neighborhood (Classic), 9.1 on Win32: Program Neighborhood Agent.

  - Citrix ICA 9.1 on Win32: Web interface.
- Thin clients:

  - Thin terminals with Windows XP Embedded operating system and the Citrix ICA Client 8.0. ICA 8.0 - Windows XP Embedded thin client.

Reference hardware and software

The following list provides the reference hardware and software used to validate the ActivIdentity 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 (HP SAM) version 2.0.
- VPN Tunnel
- Altiris Deployment Server
- Network Switch.
  - HP Procurve 2626.
- Blade Enclosure
  - HP BladeSystem PC Blade Enclosure
- Blade PCs
  - HP blade PC running Microsoft Windows XP SP2 w/HPSAM blade service installed.
- Clients
  - HP Compaq t5720 thin client running Microsoft Windows XPe w/HP SAM Windows XPe-based service installed.
  - HP Compaq dc7700 running Microsoft Windows XP w/HP SAM Windows XPe-based service installed.

- Smart Card Readers
  - HP standard USB Smart Card Keyboard. Go to **http://www.hp.com** for driver support available with sp31137.exe (driver 4.30.0.1) or greater.

    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).
- Windows Enterprise 2003 Server RC2.
  - Configured as DNS, DHCP, IIS, CA and secure Web site server.
- Entrust client software: ActivClient supports the following Entrust products:
  - Entrust Entelligence™ Desktop Solutions 6.1 SP1
  - Entrust Entelligence Desktop Solutions 7.1
  - Entrust Entelligence Security Provider for Windows 7.0 SP3
  - Entrust Authority™ Security Toolkit for Java Version 7.0
  - Entrust File Toolkit 6.0 SP4
  - Entrust Session Toolkit (GSS-API toolkit for C) 6.0 SP4
  - Entrust Authority™ Security Manager Administration 7.1
  - Entrust Authority Administration Services 7.0
  - Entrust TruePass™ 8.0
  - Entrust Entelligence Security Provider for Windows 7.1
  - Entrust Java Toolkit 7.1.

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**.

Client Software Configuration

Installing ActivClient PKI Only

The Setup Deployment chapter of the Resource Kit provided by ActivIdentity discusses how to deploy ActivClient using standard methods.

The ActivClient PKI Only 6.0 allows the user (based on privileges) or the Administrator to change and verify the PINs, view card and system information, and register certificates. HP does not support and has not validated any ActivClient Enterprise class smart card provisioning solutions. For administrative smart card provisioning, HP recommends that you contact ActivIdentity for a list of Enterprise class life cycle management tools and access to their ActivClient Resource Kit to provide administrative management of client smart card usage. Any client-based provisioning software installed may require write filter commit on the HP thin client.

An illustration of Administration provisioning is initializing a card and having to keep track of the "unlock code" manually or having to manually download certificates to the card. The remainder of this guide outlines installation of minimal client options, ActivDirectory management of certificates, and assumes the Administrator manually tracks card unlock codes. For large scale rollout or deployment options, please consult with ActivIdentity during your software purchase or consider the ActivClient to be managed by the card user (a client-user based provisioned model would require normal setup.msi installation or modification to the minimal installation parameters listed below for greater client-based card management control).

These identified services typically get installed with defaults provided with a standard ActivClient PKI Only.msi installation:

- Pin-initialization
- Advanced Configuration Manager
- Advanced Diagnostics
- Digital Certificates Services (node)
- Entrust Entelligence Desktop Solution Support
- User Console
- Troubleshooting

Installation of ActivClient PKI Only 6.0 requires changing the thin client RAMDisk size to 64MB as well as changes to the Windows environmental variables on an thin client. These changes must be made from an administrative privileged account.

NOTE: During the software installation, the reader should not contain a smart card.

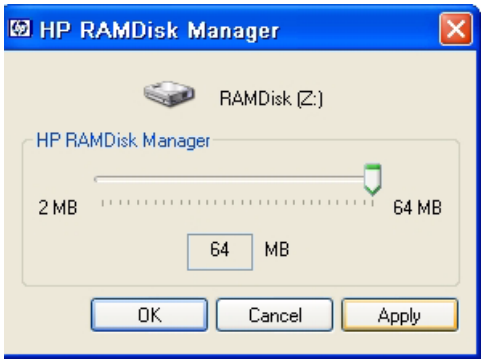
NOTE: Close all open Windows programs and applications.

NOTE: You will be prompted to reboot after clicking **Apply** to the RamDisk size change. Commit (EWF) data to the volume after completing the installation or changes will be lost on the next reboot.

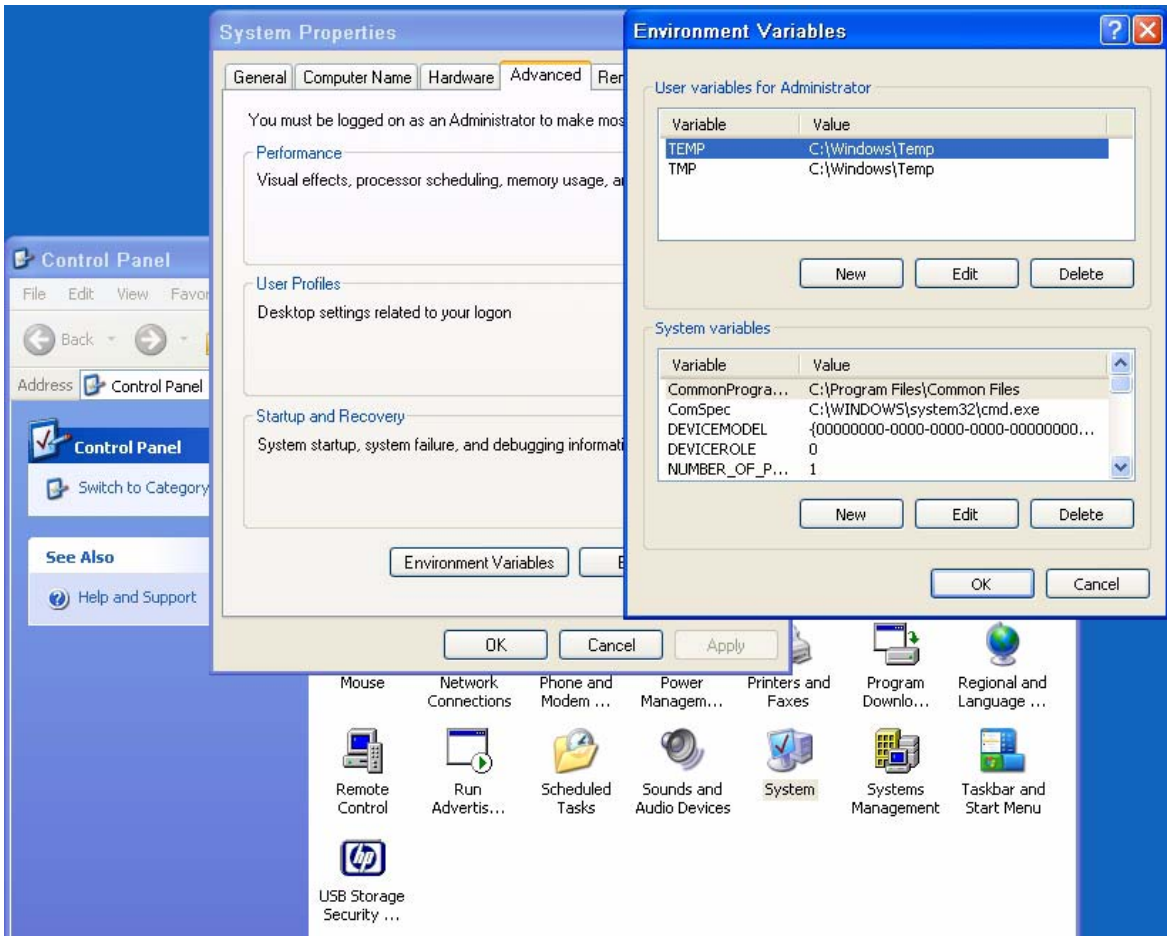
NOTE: HP deployment solutions such as Altiris client manager do not require RAMDisk size adjustments or modification of environmental variables.

As mentioned above, the first installation step is to modify the thin client's RAMDisk size from default settings to 64 MB. Make note of the default setting so that it can be restored after installation is complete.

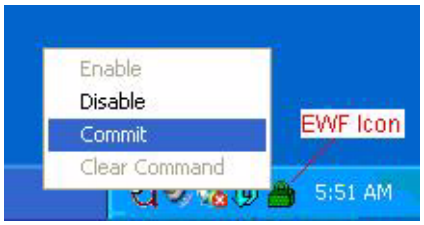
To change RAMDisk size, click **Start > Control Panel > HP RAMDisk Manager**.



Next, modify the thin client TEMP and TMP environmental variables to a location that can support the .msi user installation package size. To change environmental variables, click **Start > Control Panel > System Properties > Advanced** tab **> Environmental Variables.**



Once the environmental variables have been changed, right-click on the EWF icon on the taskbar and select **Commit**.



NOTE: The environmental variables should be changed back to default settings after installation package has been installed, and then the write filter changes must again be committed.

Installation of ActivClient base services and CSP is required on the client for smart card support. Due to t5720 flash drive space constraints, recommended minimum installation parameters are outlined by using the following install command-line parameter (please consult ActivIdentity Resource Kit documentation for further customizable install parameters and deployment capabilities):

```
msiexec /i "ActivClient PKI Only.msi" BASEREQ=1 CSPREQ=1 DEVICEREQ=1 KEY-
SIMREQ=1 RAANDOTPREQ=1 OUTLOOKREQ=-1 PKCSREQ=-1 PCMCIAV2REQ=-1 USBV2REQ=-
1USBV3REQ=-1 ADVCONFMANREQ=-1 ADVDIAGREQ=-1 CMSREQ=-1 PIVAPIREQ=-1 ACSAGEN-
TREQ=-1 USERCONSREQ=-1 AUTOUPDATEREQ=-1 DOCREQ=1 DOCCACREQ=-1 PININITTOOL-
REQ=-1 PINCHANGETOOLREQ=-1 TROUBLESHOOTING_ENABLED=1
```

The previous command includes installation of:

- Base Services
- Microsoft CAPI support
- Device Drivers
- Remote Access & OneTime Password Services

Applying an advanced configuration default template to clients that meets Government Smart Card Interoperability Specifications (see **http://smartcard.nist.gov/** for details on GSC-IS) is possible via group policy objects, registry editors, or ActivIdentity Advanced Configuration Manager software included with ActivClient PKI Only software CD. For specifics about implementing default templates, refer to the section about product customization in the *ActivClient Customization and Deployment Guide* included in the ActivClient Resource Kit.

NOTE: To remove the ActivIdentity software from an HP Compaq t5720 Thin Client, you must use `MSIEXEC /x "ActivClient PKI Only.msi"` command. Manual execution of the MSI or through the product CD requires usage of add/remove programs which is not available on HP thin client systems.

Initializing the smart card

Use the following procedure on blank smart cards or cards which contain a standalone profile that need to be re-initialized. To initialize your PIN using the PIN Initialization Tool:

1. Go to **Start > Programs > ActivIdentity > ActivClient** and select **PIN Initialization Tool**.

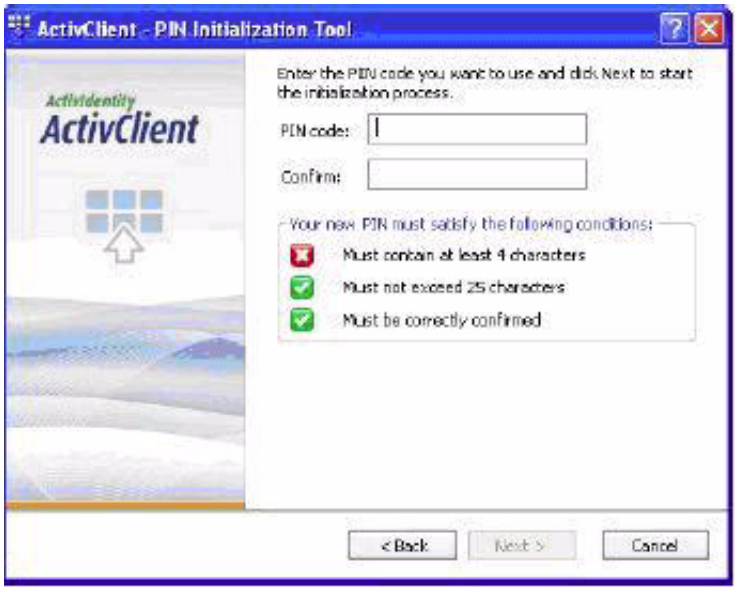
   -or-

   Right-click the ActivClient Agent icon located on the Windows taskbar and select **PIN Initialization Tool** from the right-click menu.

2. Follow the PIN Initialization wizard.

   Note: PIN Initialization tool profile. ActivClient also supports a profile specifically created for the PIN Initialization tool

3. Enter your PIN code, confirm it, and then click **Next**.



NOTE: The PIN code must conform with the PIN rules displayed by the tool. All the rules must display a green check for the PIN Initialization Tool to let you move forward.

4. In the case of standalone smart cards (with an unlock code), you must enter a PIN or unlock code. When the initialization is complete, the Finish window is displayed.

5. In the case where an unlock code is displayed, write it down in a secure location and click Finish to close the window.

NOTE: If the card is already initialized, the following warning message is displayed:

```
ActivClient detected that your card is already initialized. Your card
will be reinitialized and any content present on the card (including
private keys) will be permanently deleted.
```

NOTE: CAC is a Common Access Card issued by the United States Department of Defense. Displays an expiration date for the card and the card's certificate. PIV is a Personal Identity Verification Card issued by the United States Department of Defense. Displays an expiration date for the card and the card's certificate. By design a CAC card CANNOT be initialized by the PIN Initialization tool.

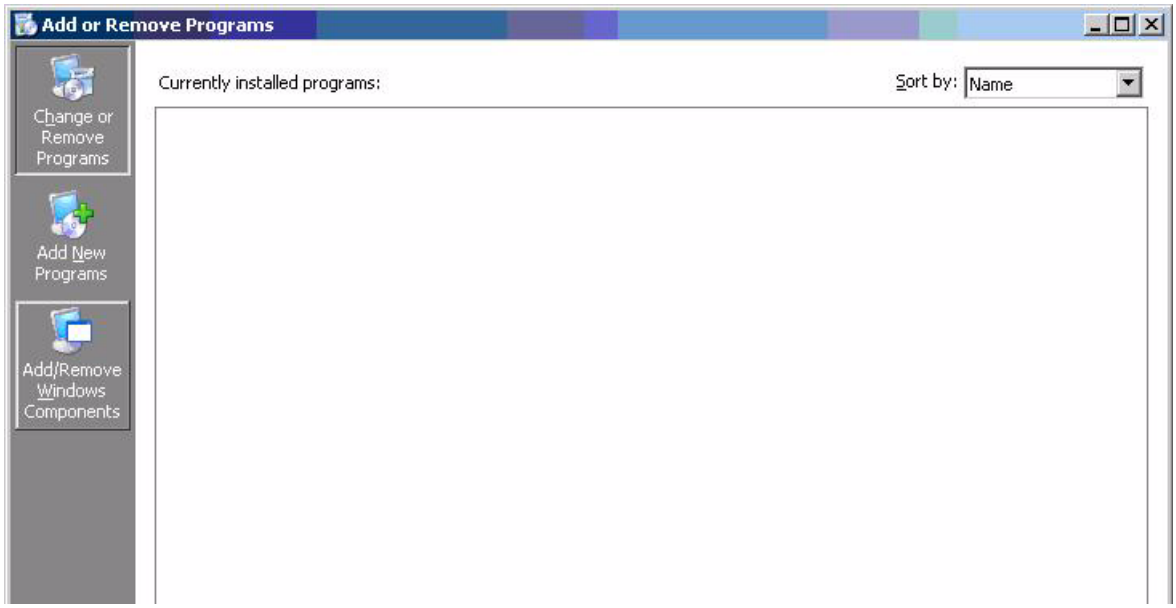
Server Software Configuration

Installing Microsoft Certificate Services

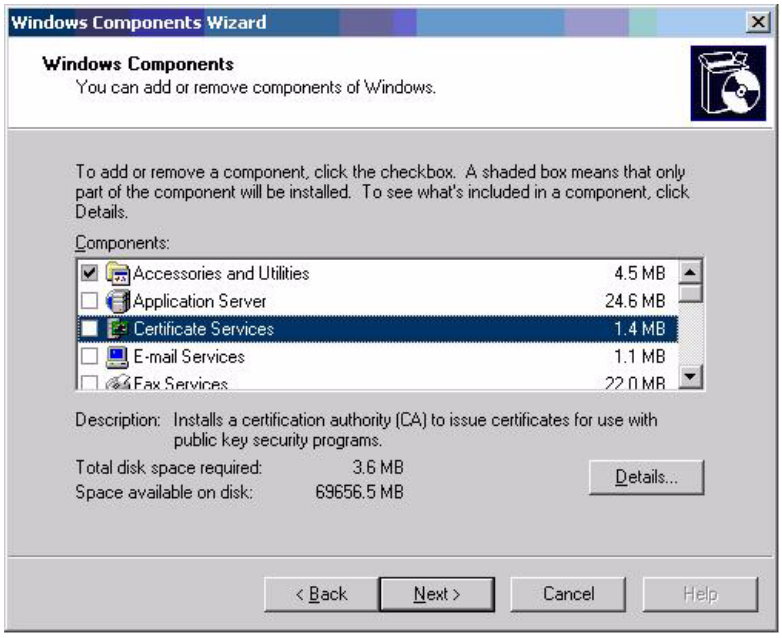
Role based administrative features included in Windows Server 2003 can be used to manage and maintain digital certificates via the Certification Authority (CA). The CA can be used by a user or administrator to provision a smart card.

To install Microsoft Certificate Services for use as a certificate authority, please perform the following:

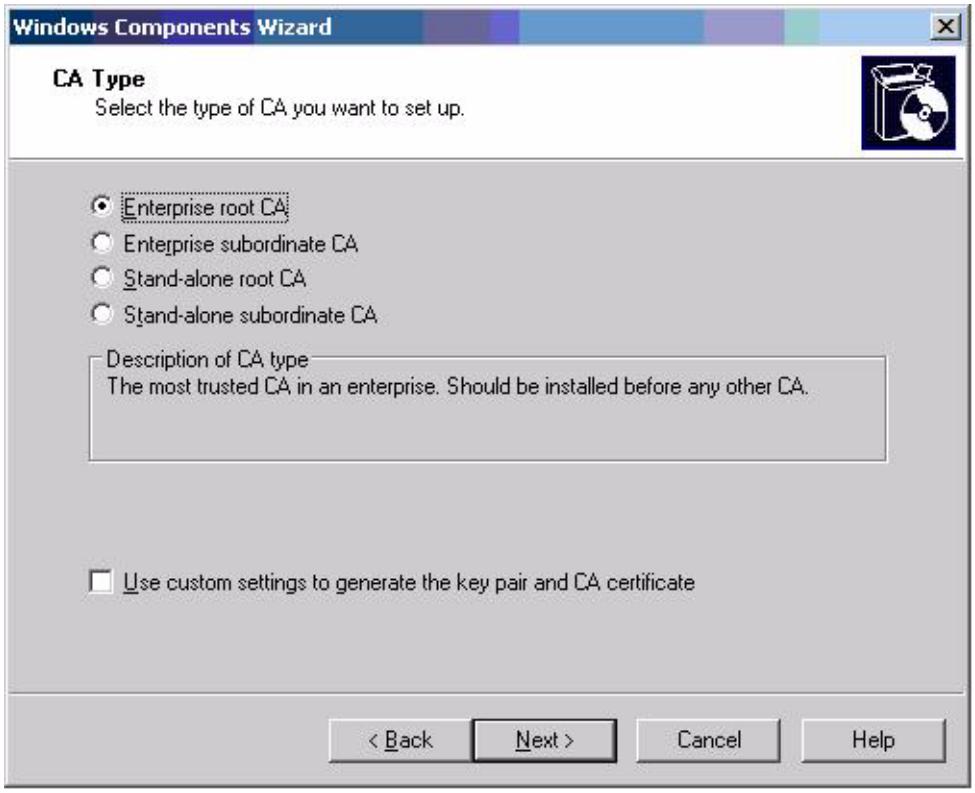
1. Click **Start > Control Panel**.
2. Select **Add or Remove Programs**.
3. In the left panel, select **Add/Remove Windows Components**.



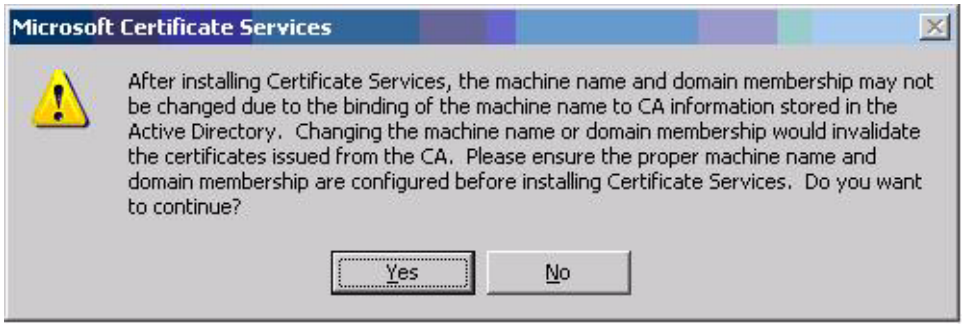
4. Click **Certificate Services**, and then click **Next**.



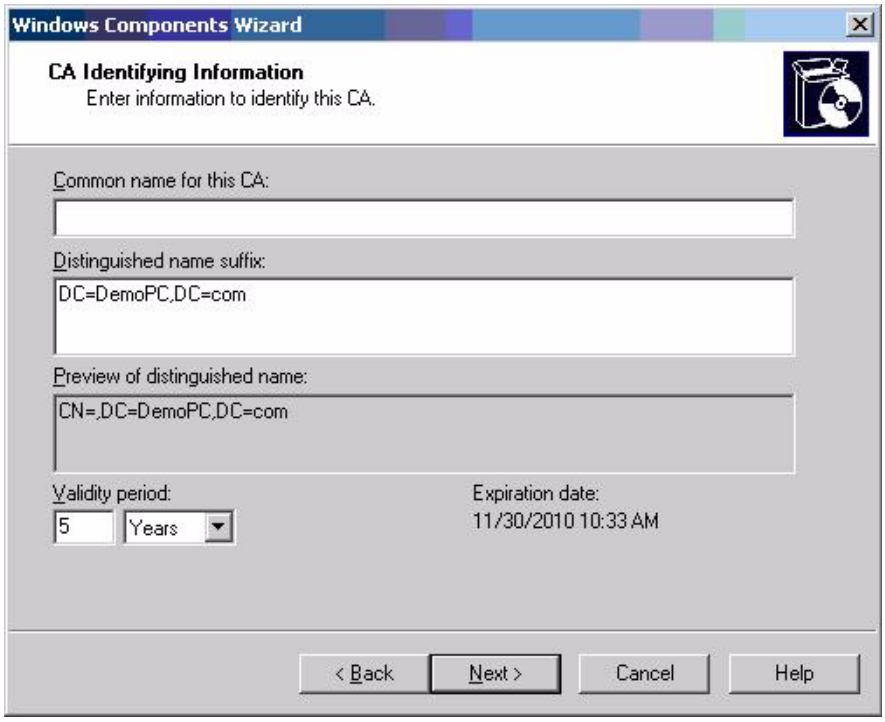
5. Select **Enterprise Root CA**, and then click **Next**.



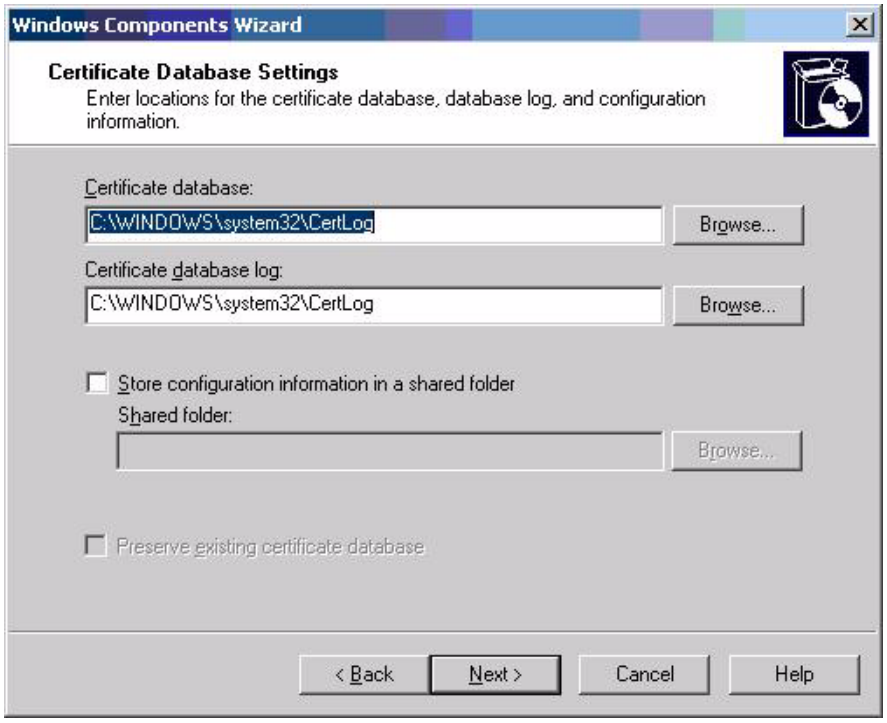
6. Click **Yes** to accept the warning.



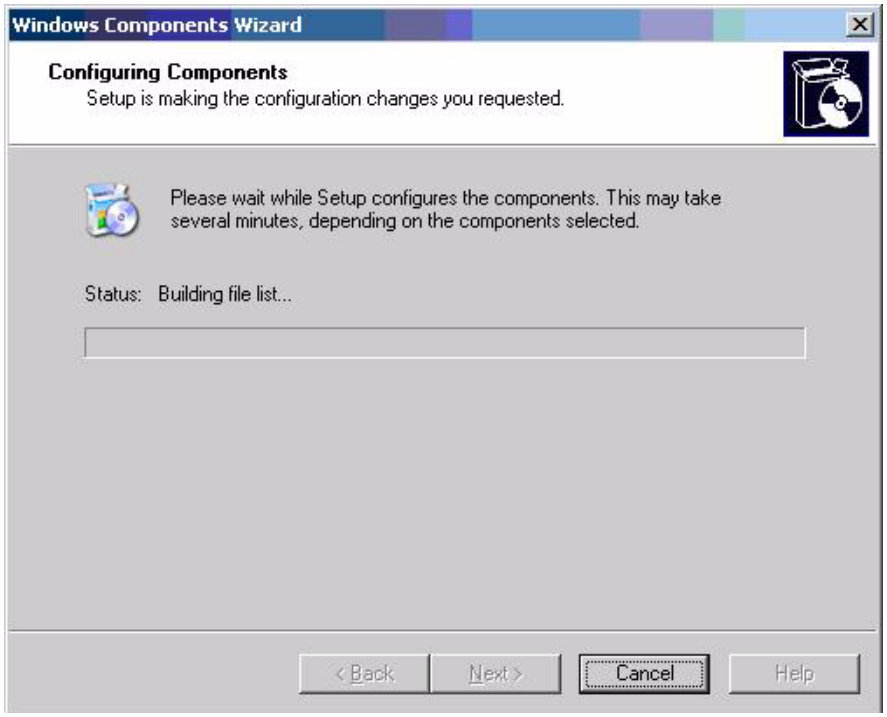
7. Type a **Common name for this CA**, and then click **Next**.



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



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.

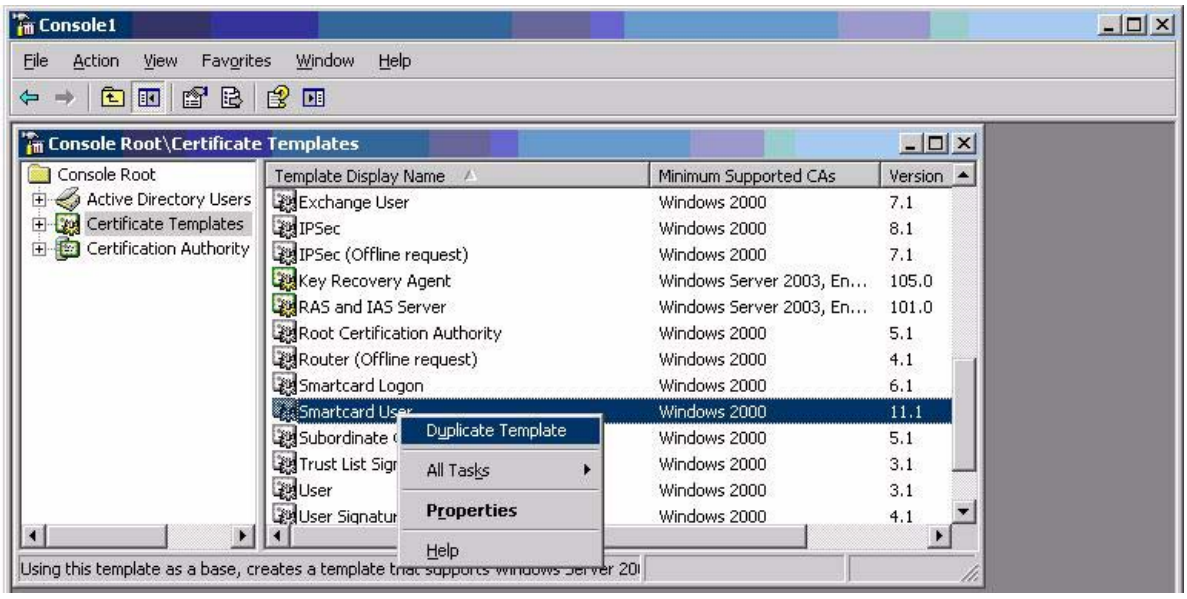
Configuring a Certificate Authority (CA) service

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.

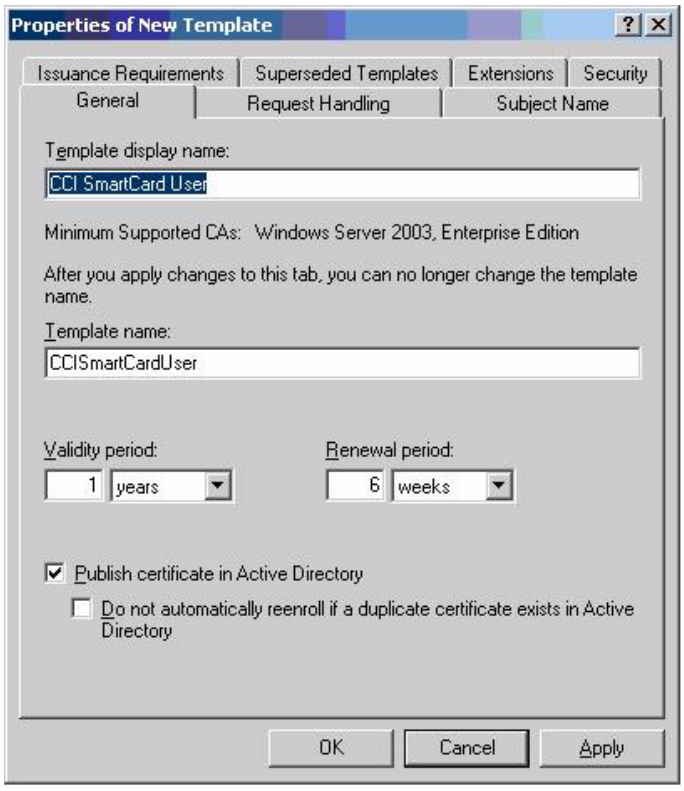
After you install the CA service, perform the following configuration steps:

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.

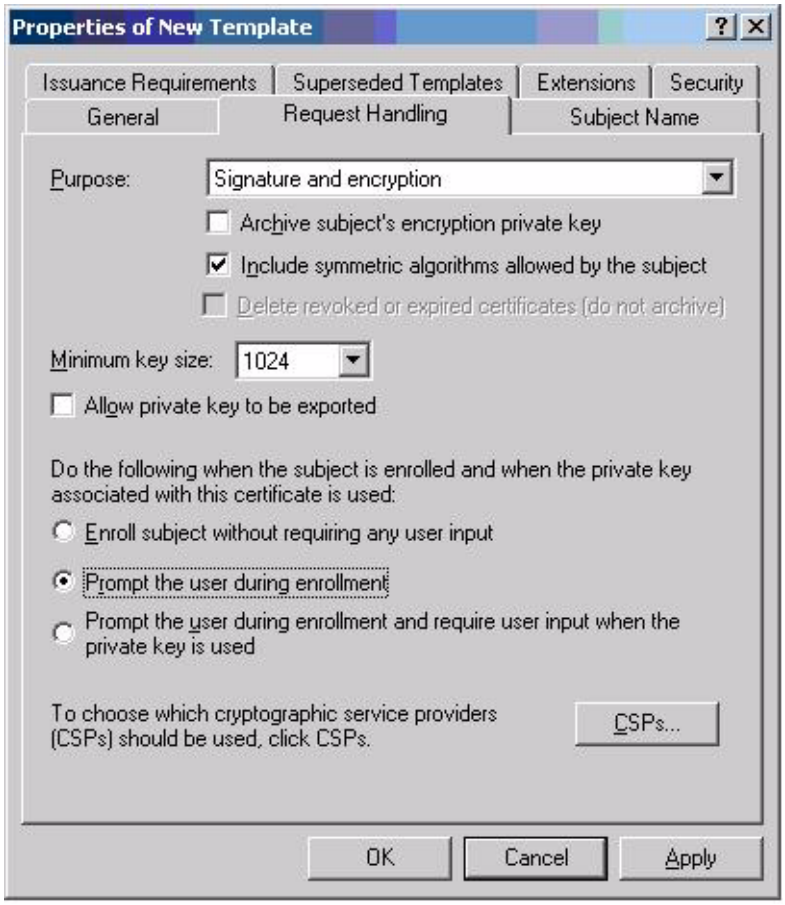
3. Create a duplicate template by right-clicking on the Smartcard Logon certificate template, and then selecting **Duplicate Template**.



4. Type a name for the new template in the **Template Display name** box. For this example we will use the template name of CCI Smartcard User. This template will be referred to for the remainder of this paper.

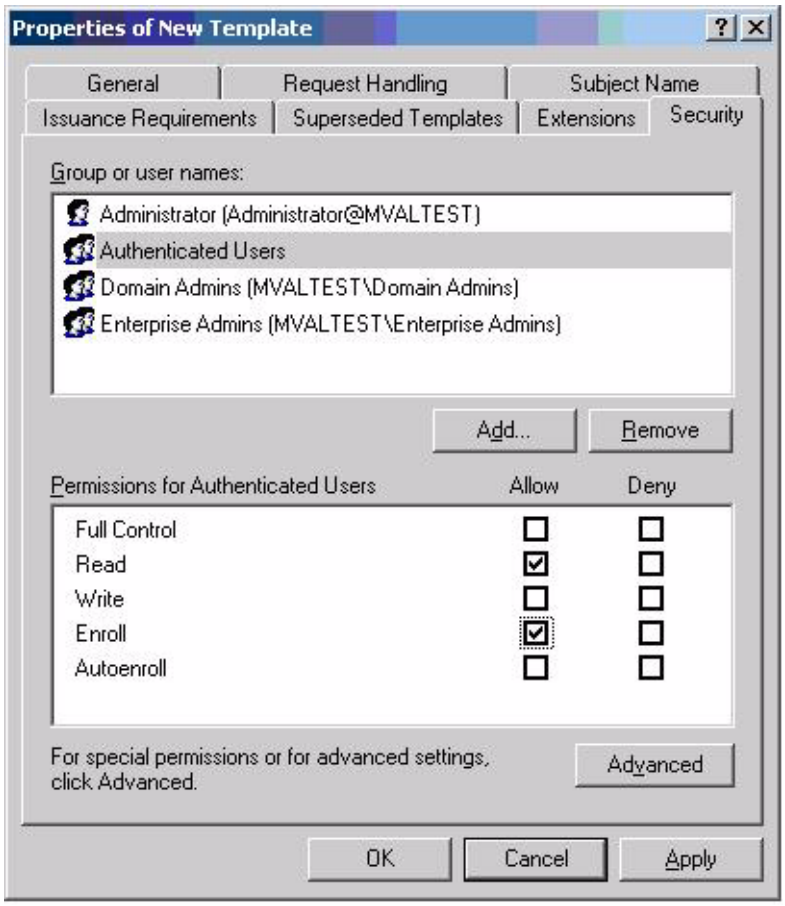


5. Click the **Request Handling** tab.



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.

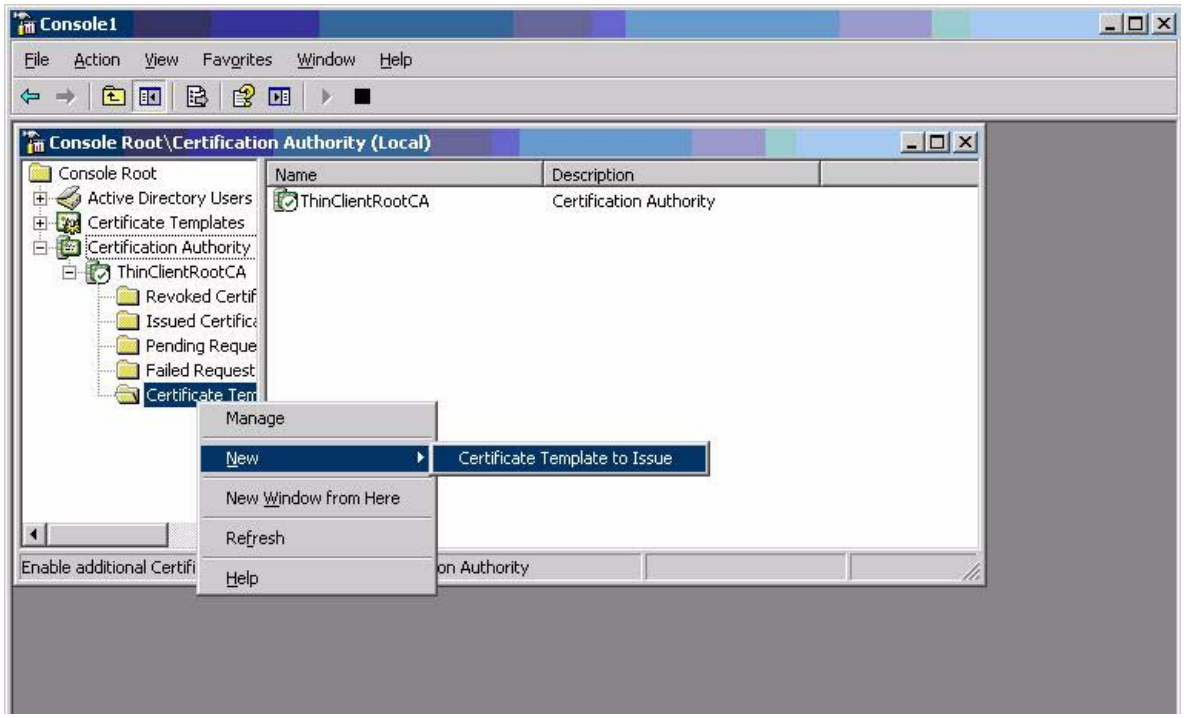
11. Copy the *CCI SmartCard User* certificate template into the **Certificates Templates** folder under the certificate server.

    a. Expand the **Certificate Authority** object in the MMC you created in step 1.

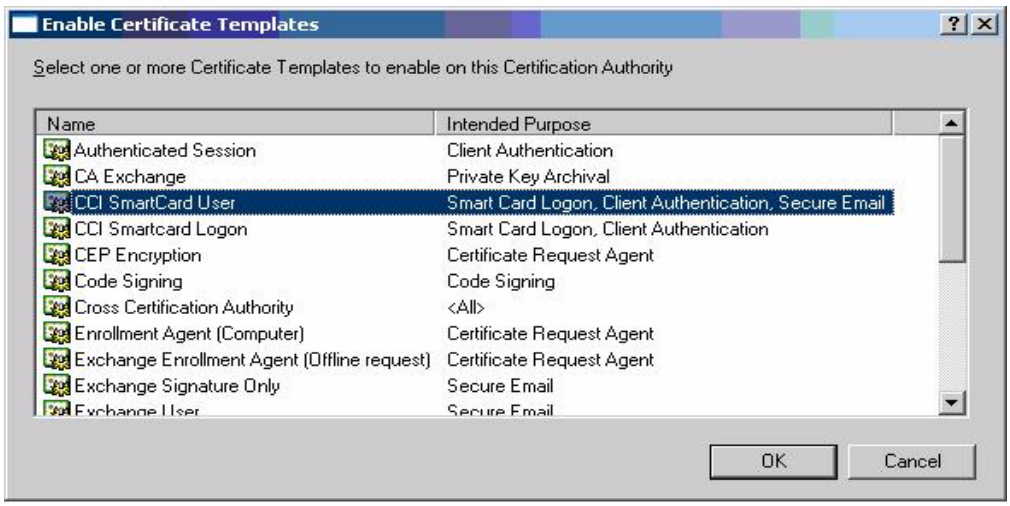
    b. Expand your CA name.

    c. 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

ActivClient 6.0 PKI Services support Digital certificate-based logon to Windows 2000, Windows XP Professional, and Windows Server 2003. The Services also support:

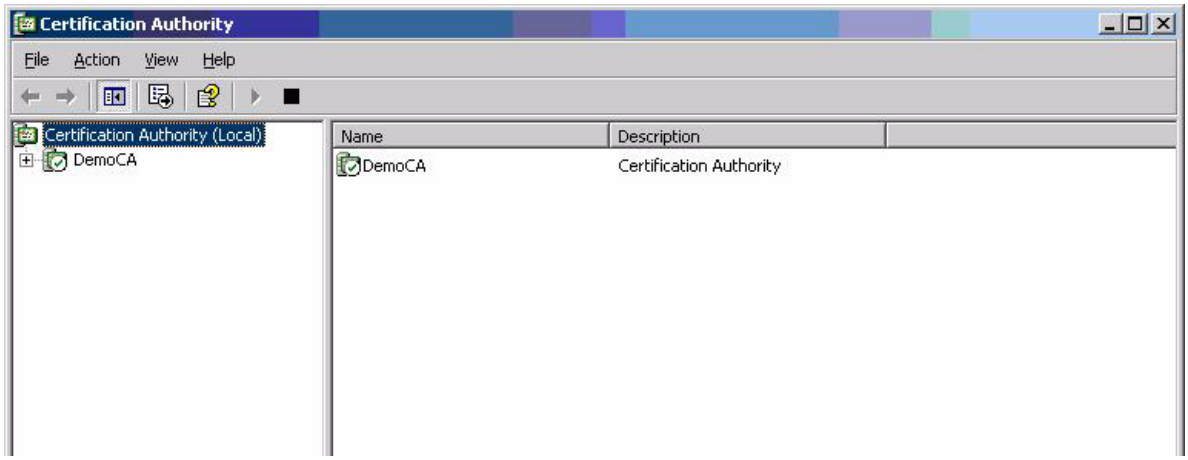
- The ability to log off user and lock workstation on smart card removal.
- Automatic certificate registration to Windows on smart card insertion and optional removal on smart card removal.
- Secure email: Email signature, encryption/decryption

Digital Certificate Services provides:

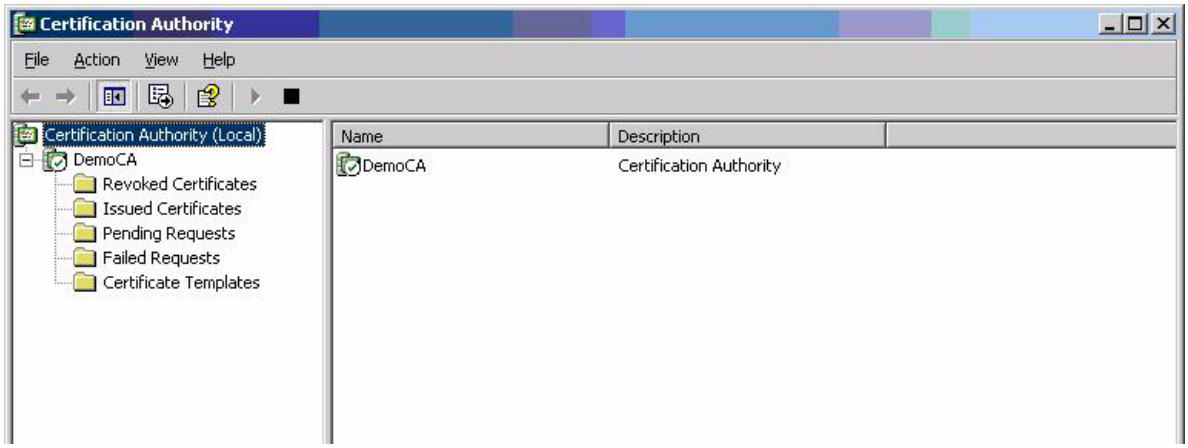
- Secure Browsing: Client Side PKI Authentication for SSL sessions
- Microsoft CAPI support
- Microsoft Outlook Usability Enhancements
- Firefox, Thunderbird, Mozilla and Netscape support
- PKCS#11 Support
- Entrust Entelligence Desktop Solution Support

To configure a CA to issue a smart card user certificate:

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



2. Expand the defined CA.

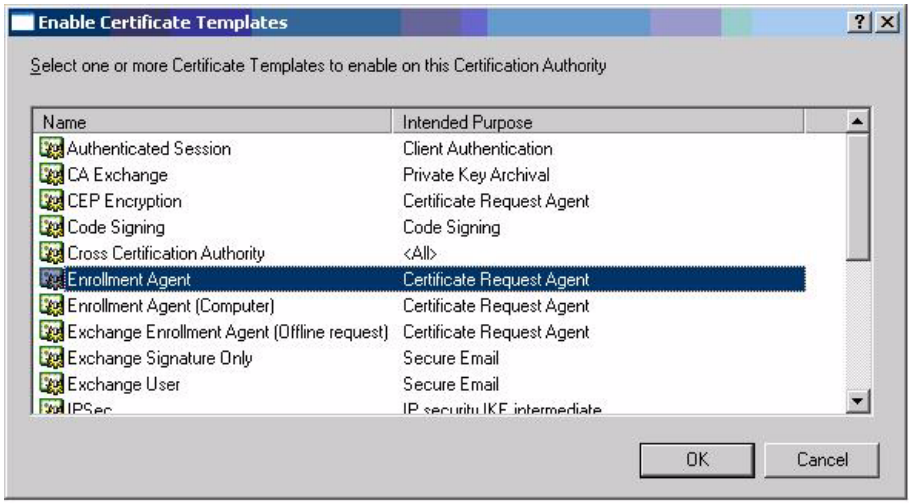


3. Right-click **Certificate Templates**, and then select **New**.

   a. Select **Certificate Template to Issue**.

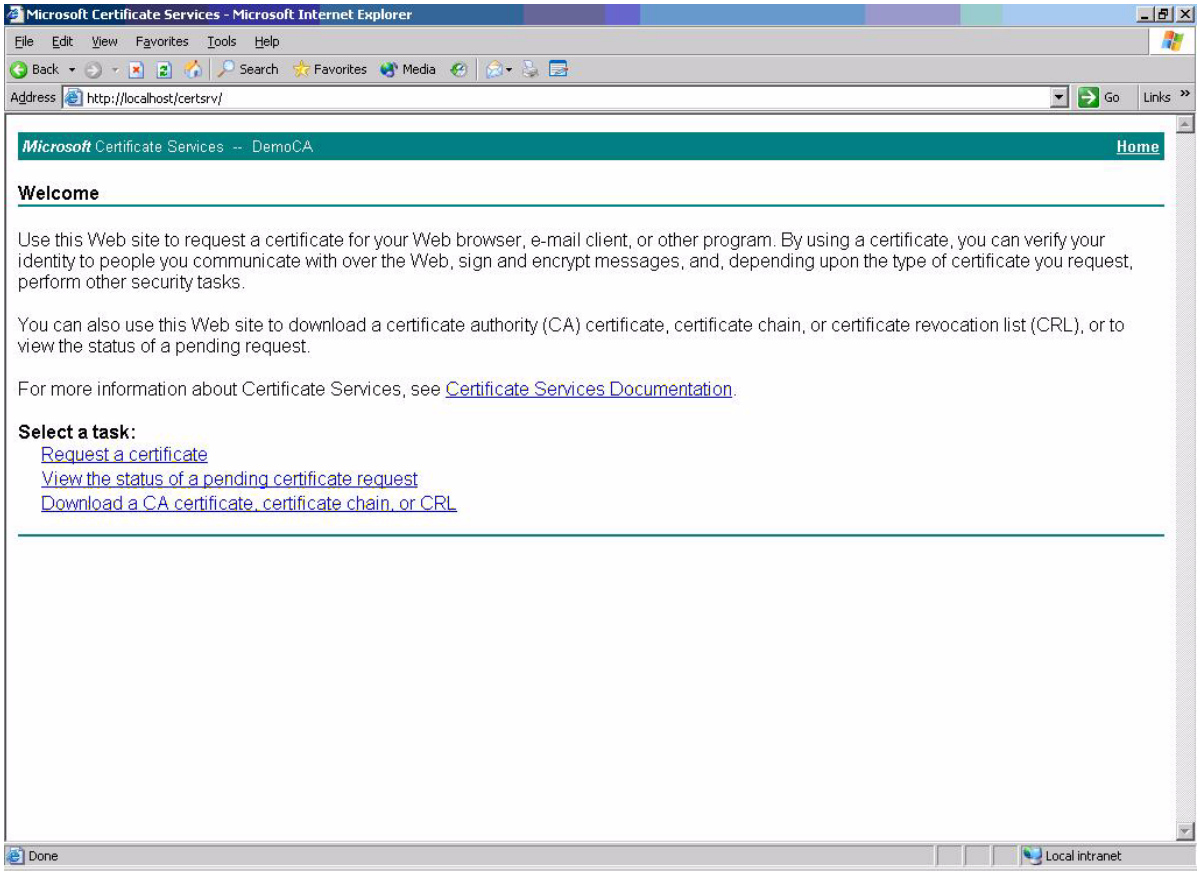
   b. Select **Enrollment Agent.**

   c. Select **OK** to add.

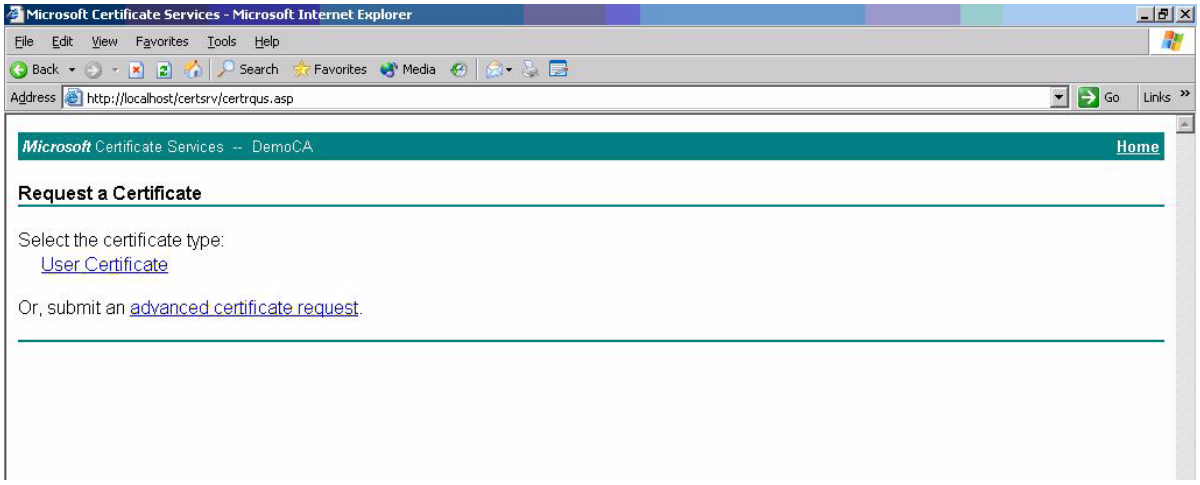


4. Launch Internet Explorer and browse to **http://localhost/certsrv**.

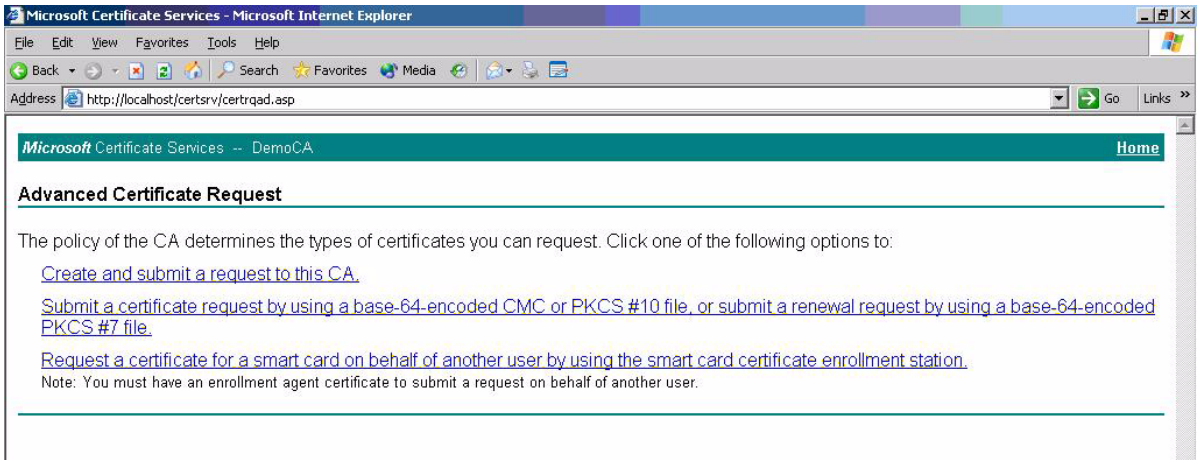
5. Under **Select a task**, select **Request a certificate**.



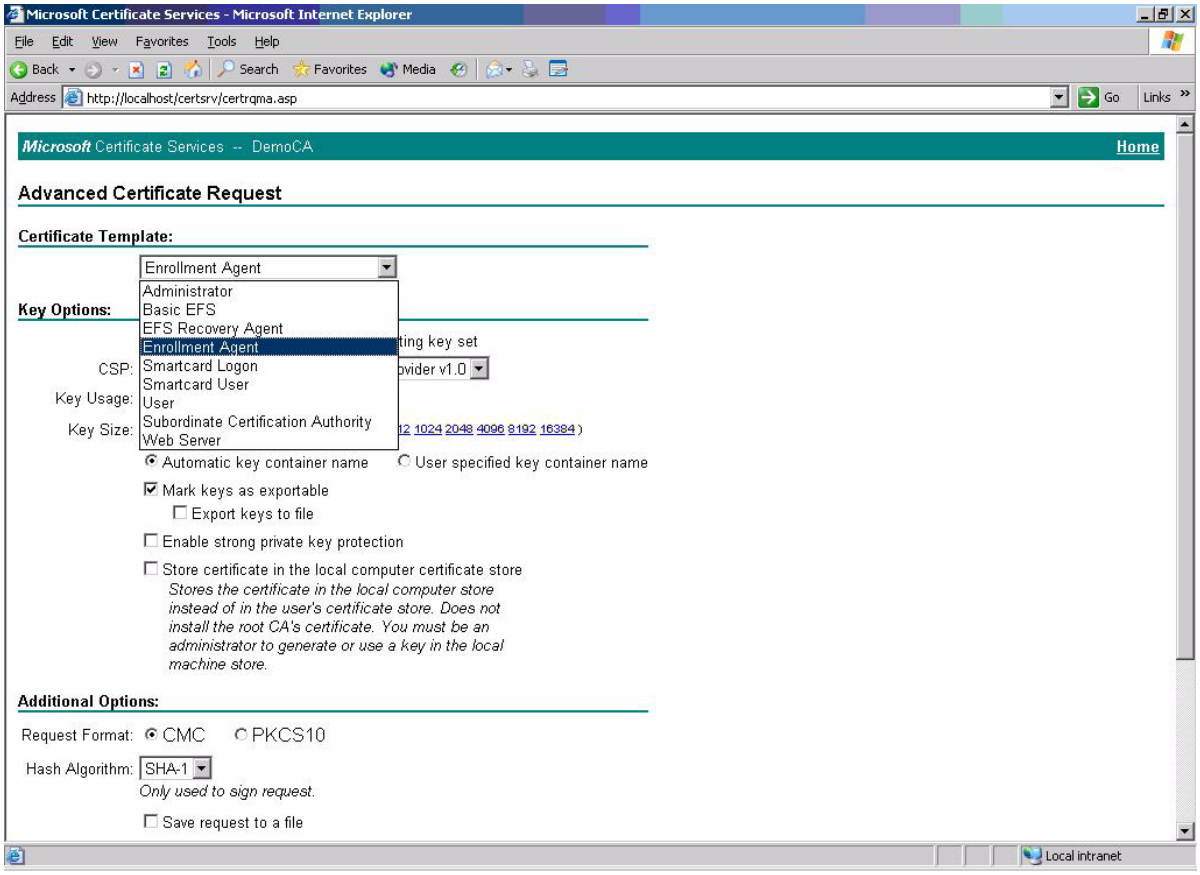
6. Select **advanced certificate request.**



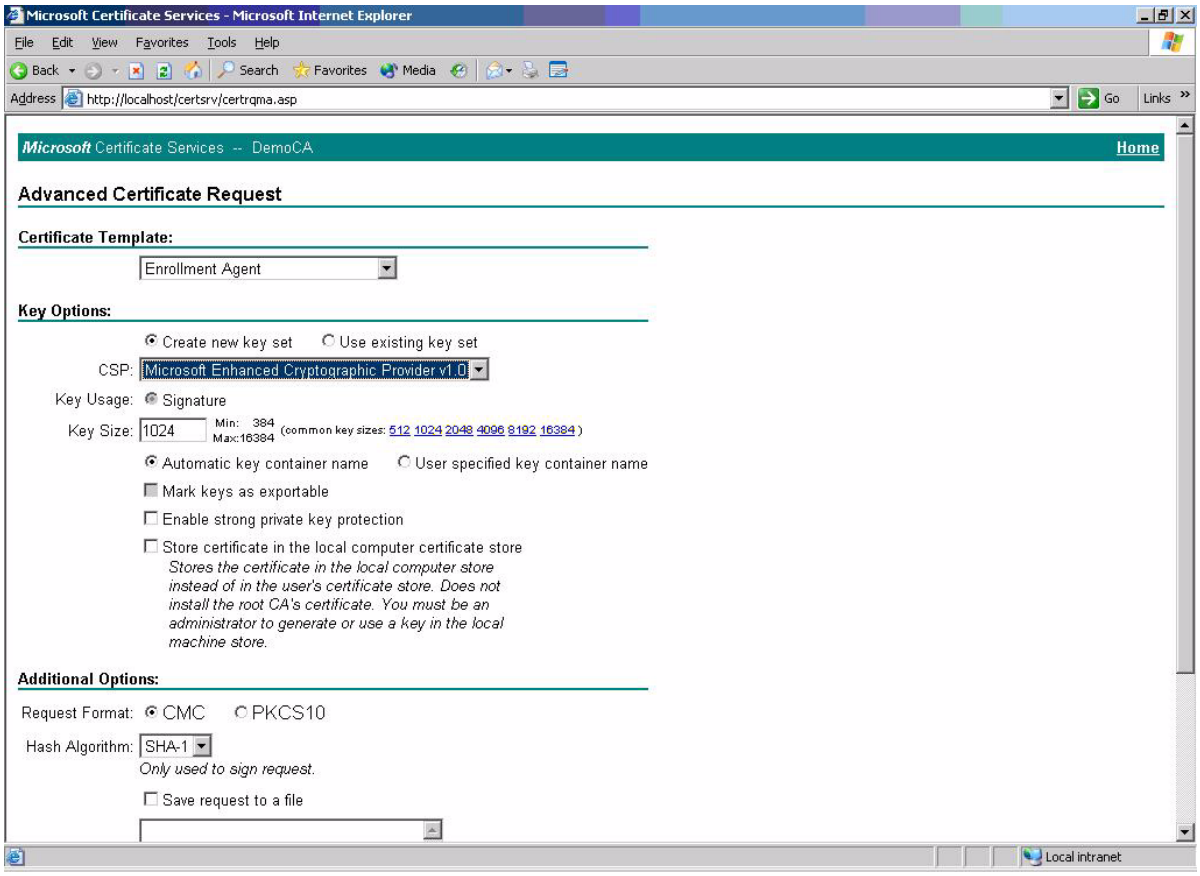
7. Select **Create and submit request to this CA**.



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

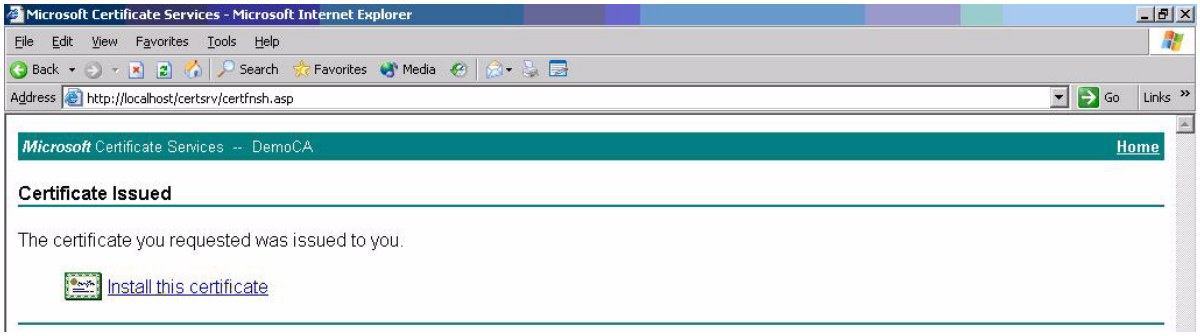


9. Verify Enrollment Agent Settings in the **Key Options** section as follows:
   - **Create new key** is selected
   - Microsoft Enhanced Cryptographic Provider v1.0
   - Click **Submit**.
10. Accept default settings under **Additional Options**.



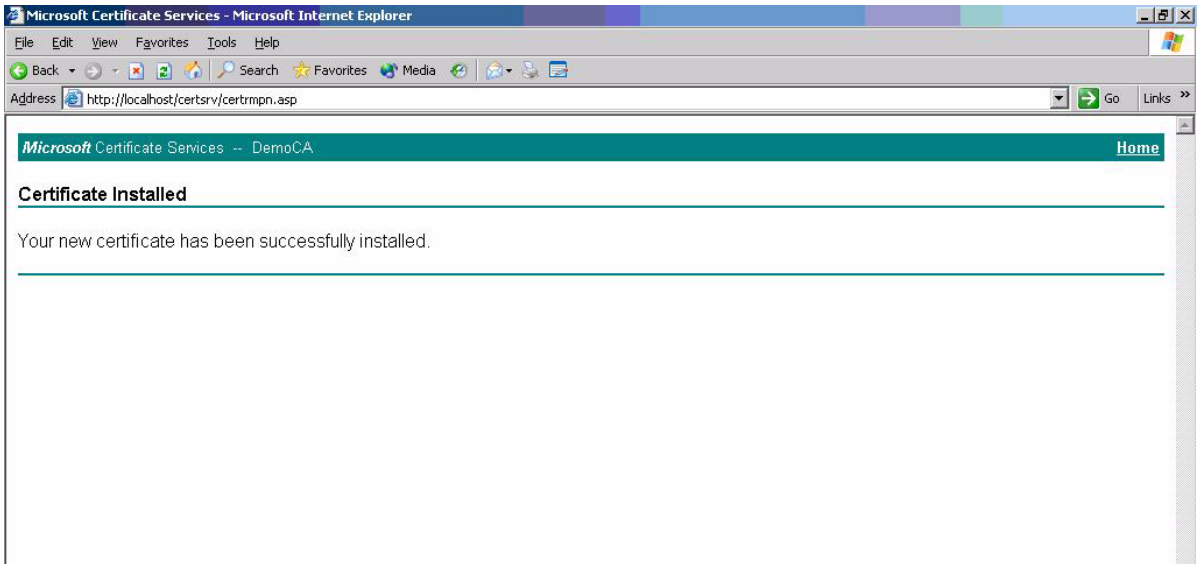
11. If a warning message displays about a potential scripting violation, press Yes to continue with the certificate request.

12. Install the Enrollment certificate requested.



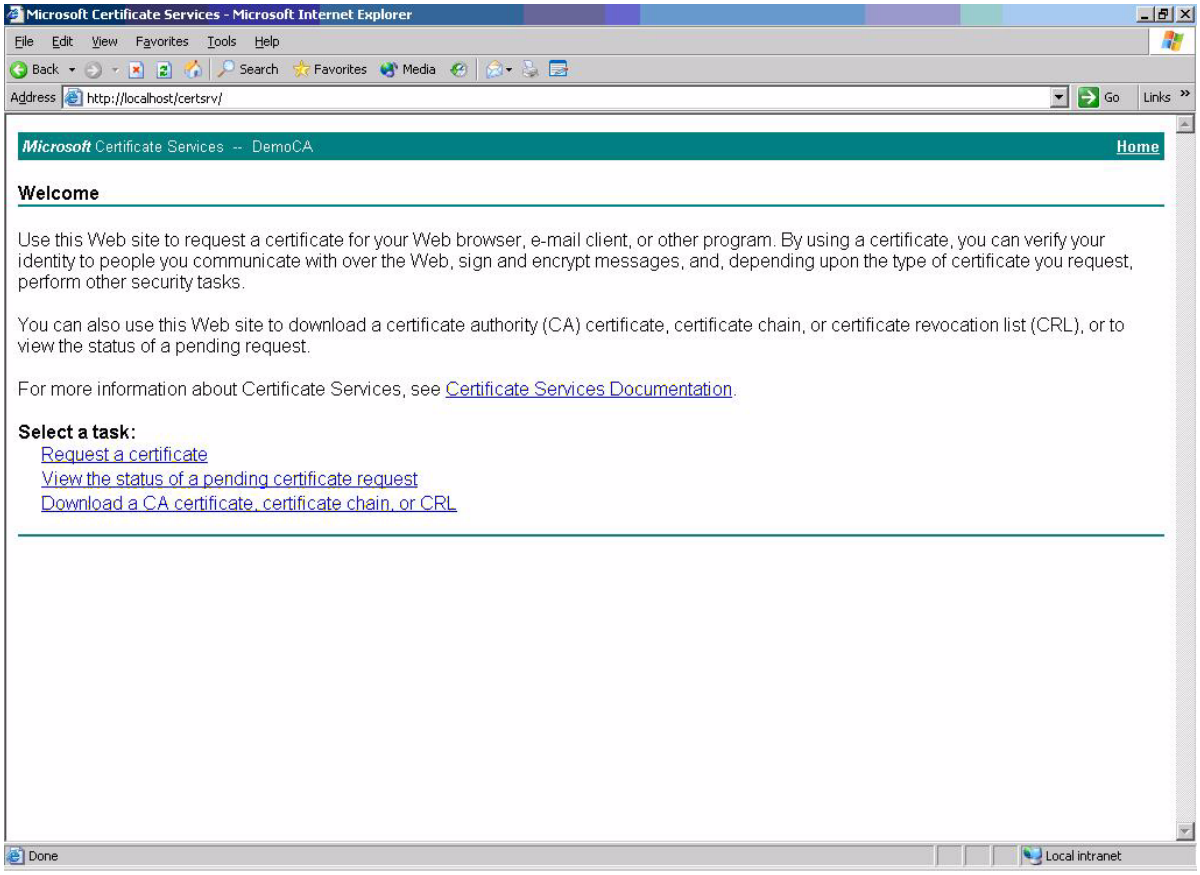
13. Select **Yes** to Potential Scription Violation.

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

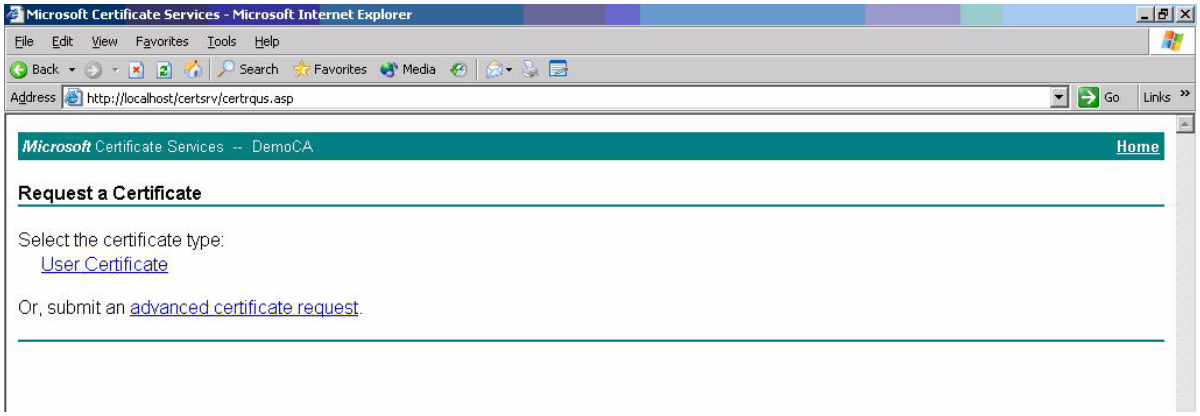


Manually issue Smart Card User Certificate

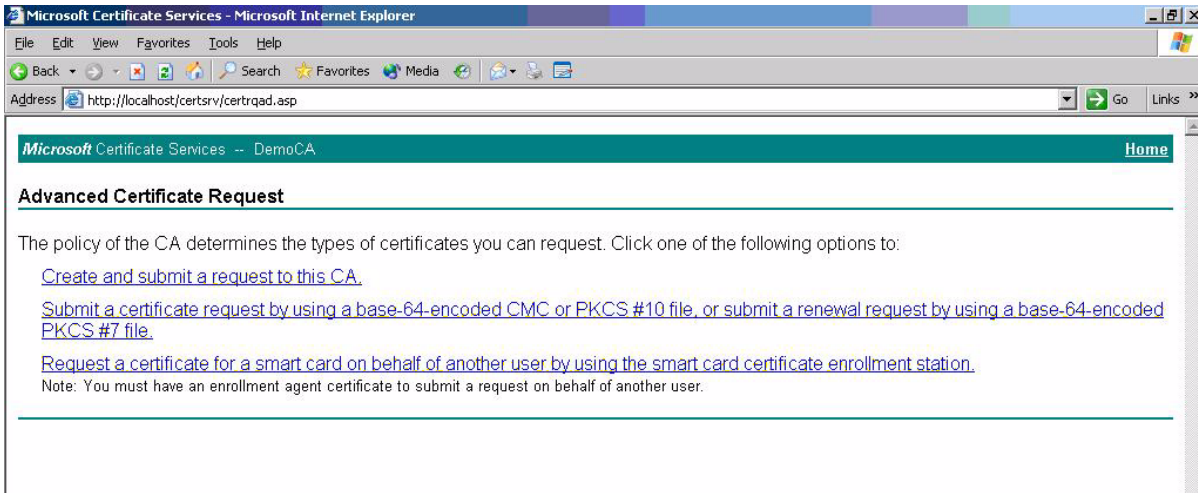
1. Launch Internet Explorer and browse to **http://localhost/certsrv**.
2. Select **Request a certificate.**



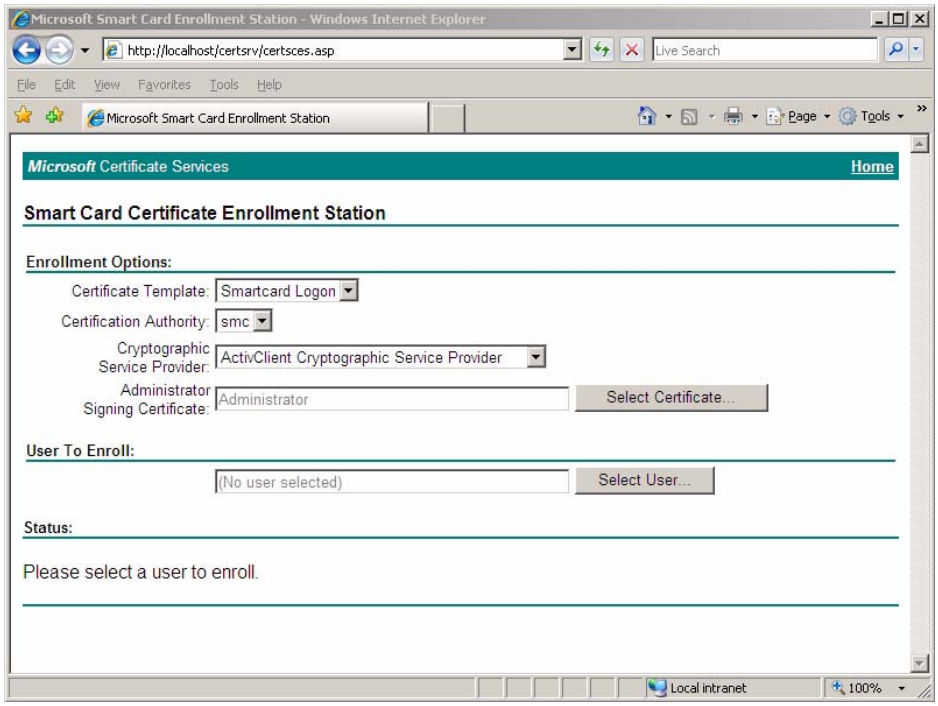
3. Select **advanced certificate request.**



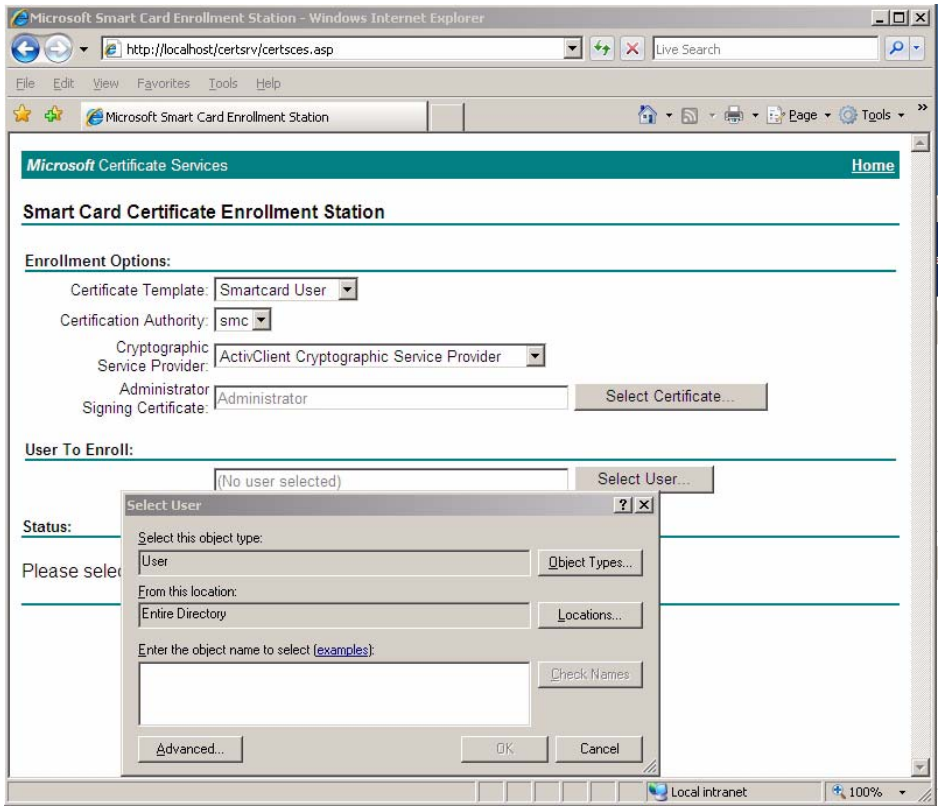
4. Select **Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.**



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

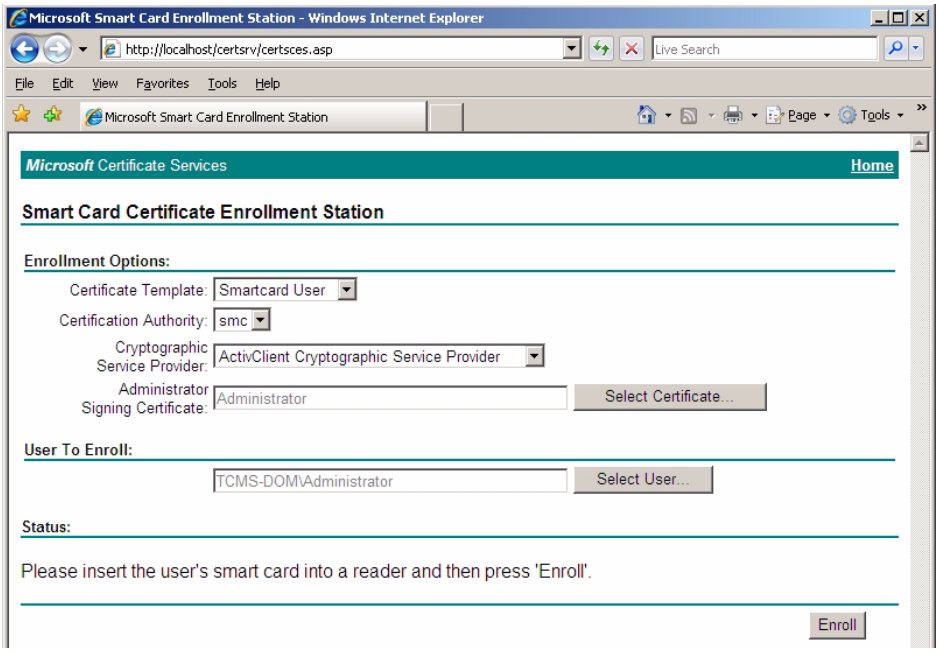


6. Define the user to enroll by clicking **Select User.**



NOTE: ActivClient Libraries may report a container error message when used for secure logon purposes. It is important that the servers Active Directory User information contain an e-mail address on any smart card provisioned with a smart card user certificate to avoid any ActivClient secure logon error messages.

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

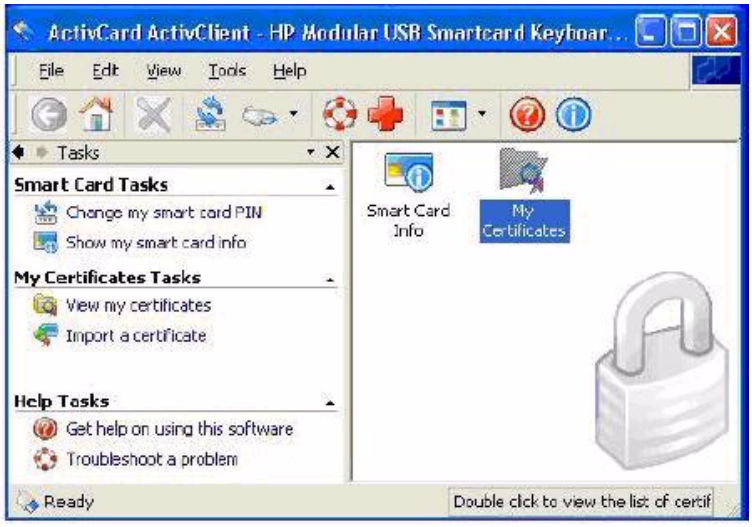


Smart Card Validation

Testing the Smart Card

To verify that the CCI SmartCard Logon certificate for the user is installed on the smart card:

1. **Click the ActivCard icon in the system tray to open the ActivClient user console.**
2. In the right pane, select the My Certificates icon. The system displays the username ID.



3. Select the username ID to view the installed certificate, which shows:
   - who it was issued to
   - who is was issued by
   - valid dates

Troubleshoot ActivClient

The Troubleshooting Wizard helps you solve any problems with ActivClient. It analyzes your system, diagnoses the problems, and then displays the results on the Diagnosis And Resolutions page.

1. Open ActivClient User Console to do one of the following:

   From the toolbar, click  .

   - or -

   From the Help menu, click Troubleshoot.

   NOTE: If you are not logged on to ActivClient, then go to the Windows Start menu, point to Programs, point to ActivIdentity ActivClient, and then click Troubleshooting Wizard.
2. When the Welcome page is displayed, click **Next**.
3. The following table lists what action to take if you have not connected to a smart card reader or you have not inserted a smart card.

If	Then	Action
You have not connected a smart card reader (or have not connected it properly)	The Please Connect Your Reader page is displayed.	Check your smart card reader connection and fix any connection problems.
You have not inserted a smart card (or have not inserted it properly).	The Please Insert Your Smart Card page is displayed.	Insert or reinsert a smart card.

4. When the Please Enter Your PIN page is displayed, type your PIN, and then click **Next**.

The following table lists what actions to take next if you do not type your PIN or the Troubleshooting Wizard is displayed:

If	Then	Action
You do not type your PIN.	With the certificates stored on your smart card, the Diagnosis and Resolutions report will not: • Test encrypt and decrypt • Digital signature • Web authentication	None.
The Troubleshooting Wizard detects a problem such as a smart card that has not been inserted or cannot be read.	The Problems Found page appears.	Proceed to step 5.

5. When the Analysis in Progress page is displayed, click **Next**.
6. If problems are detected, then the Problems found page is displayed. Click **Next**.

   The Diagnosis and Resolutions page is displayed.

   This page contains instructions on how to correct these problems. If there are a number of problems or if the instructions are long, then drag the scroll box to move through the information.
7. Follow the instructions displayed in the Diagnosis and Resolutions window, if any, then click **Finish**.

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 ActivClient PKI Only 6.0 Libraries users setups, restart the system. The system will recognize the smart card reader and will prompt you to insert your HP ProtectTools Java card.

If the user has a locked PIN, it can be unlocked by the Administrator or if the Administrator has granted the user the right to unlock the PIN. If the user does not have this privilege, he or she should contact the Administrator to unblock the PIN. The Administrator/user can unlock the PIN by entering the unlock code. However, if the Administrator/user enters three incorrect entries in an effort to unlock a PIN, the card will no longer be usable. Please check with your Administrator prior to submitting a PIN to ensure you have the proper one.

Working with ActivClient PKI Only 6.0 Libraries

Now that ActivClient PKI Only 6.0 Libraries is installed, please refer to the ActivClient PKI Only 6.0 Libraries Administration or User Guide to learn how to:

- Manage the smart cards and certificates used with ActivClient PKI Only 6.0 Libraries
- Use ActivClient PKI Only 6.0 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 ActivClient PKI Only 6.0 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.

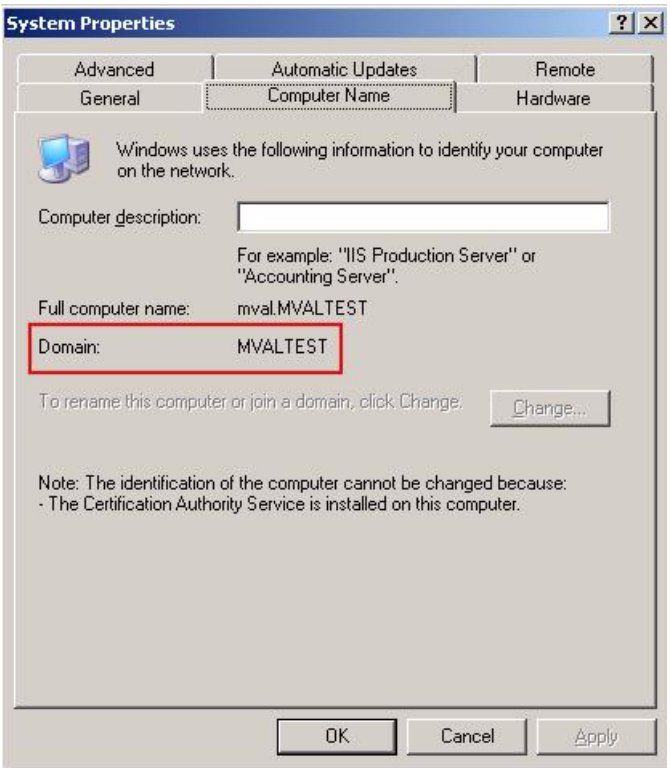
For more information about ActivCard, see **http://www.actividentity.com**.

Usage cases

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

The following steps provide instructions for performing a functional test of the SmartCard Logon certificate (assumes ActivClient PKI Only 6.0 libraries have been distributed to client blade PCs):

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



2. "Log Off" or reboot the HP blade PC.
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 SmartCard Logon certificate:

1. Log out of the RDP session.
2. Open the Remote Desktop Communications window and initiate a connection to the HP blade PC.
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

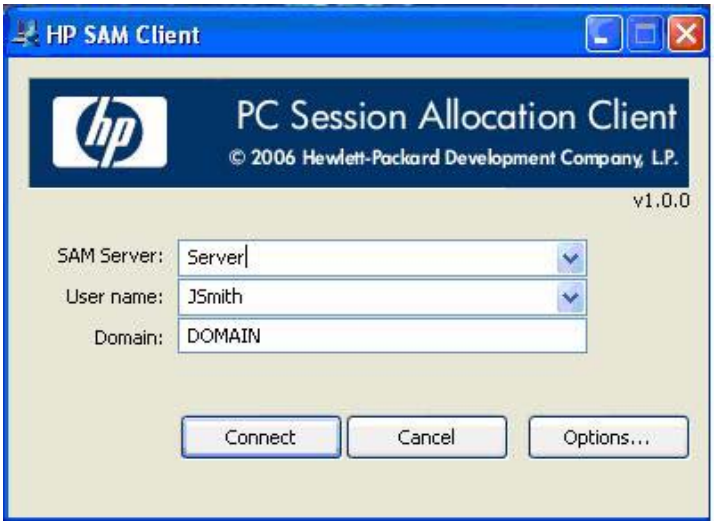
Usage case 3: User authentication from client device to HP blade PC or Active Directory Server using the HP SAM client

Supported configurations:

- Windows XP client (ActivClient optional) connecting to Terminal Server (ActivClient required).
- Windows XP client (no ActivClient; smart card reader driver required for smart card support) connecting to Windows XP (ActivClient required).
- Smart card operations are supported within an MS RDP session. Software such as Outlook is running on the remote machine but the smart card reader is on the client.
- One client accessing multiple Terminal Servers in the same session (with ActivClient running on each Terminal Server).

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

1. Log out of the MS RDP session.
2. Open the HP SAM client window and initiate a connection to the HP 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 HP blade PC or Active Directory Server.

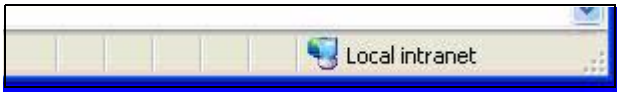
Usage case 4: Accessing secure Web site

Secure Web access means access to any Web server with SSL v3 and a digital certificate.

The following steps provide instructions for accessing a secure Web site using an ActivIdentity smart card through an HP 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 HP 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.

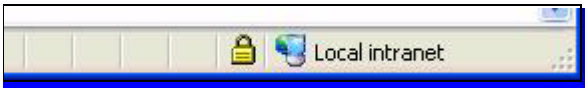
Note: Compatible with any X509 digital certificate issued by CyberTrust, Entrust, Microsoft, Netscape, VeriSign, or other leading CAs.

1. Log in to an available HP 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.

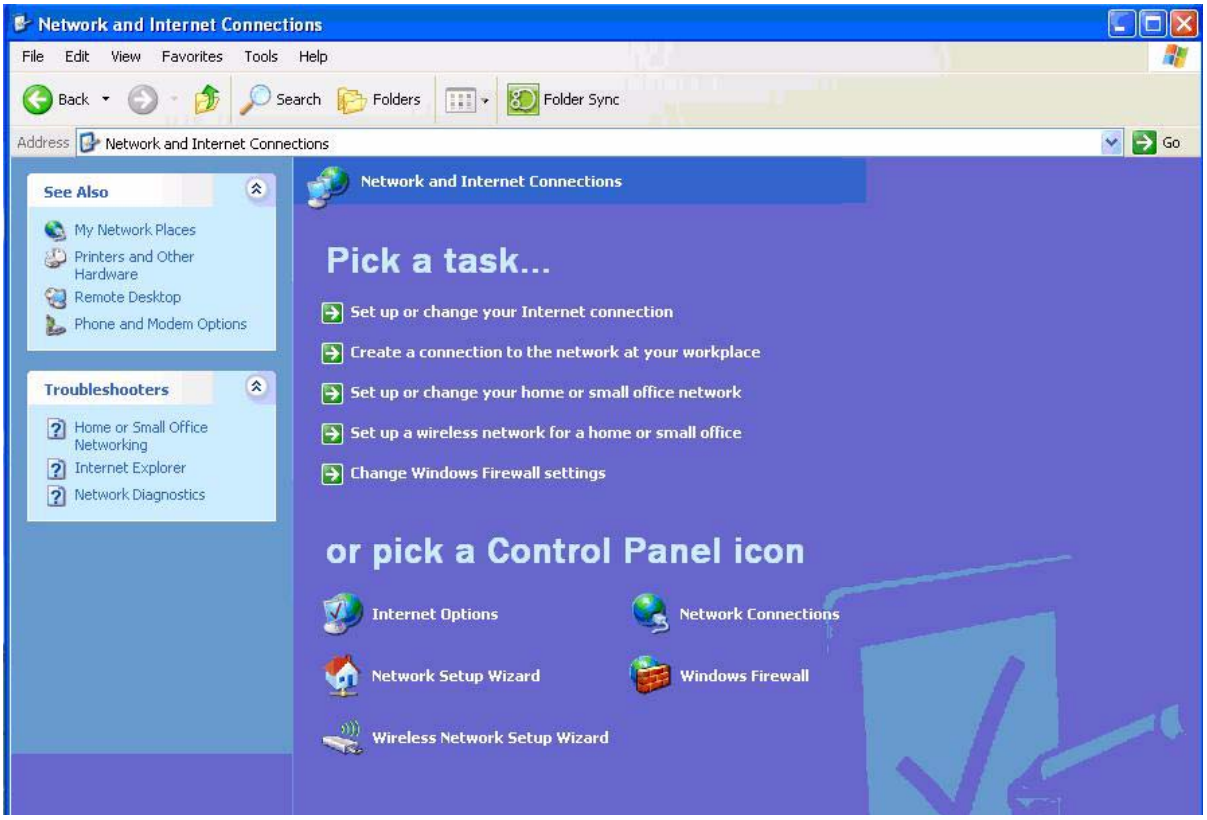


Usage case 5: User authentication using VPN through firewall to HP blade PC or Active Directory Server

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 ActivIdentity 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.

   ActivClient additionally supports Remote Access Dial-up/VPN log on with digital certificates. Please consult your ActivClient PKI Only User Guide for specific VPN hardware and software support capabilities.



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**.

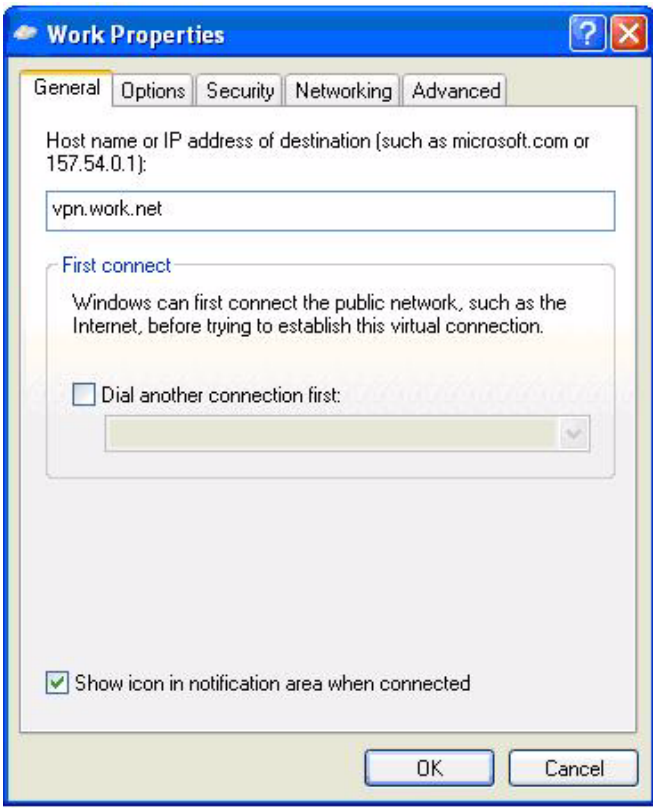
8. Select **Add a shortcut for this connection to my desktop**, and then click **Finish**.

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**.

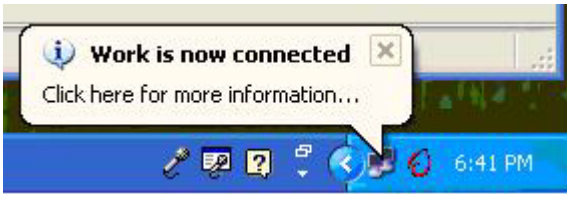


You can initiate the VPN connection after setting it up, as follows:

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

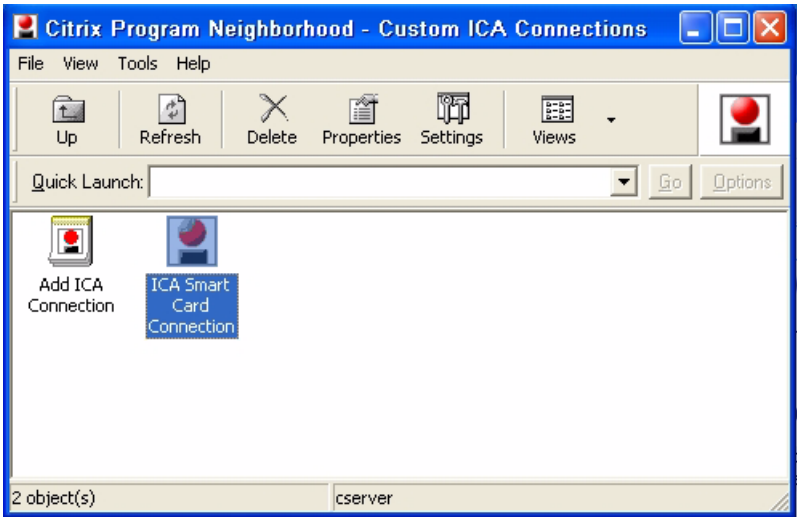
A single client can access multiple Citrix servers in the same session, with ActivClient running on each Citrix server.

Supported Citrix authentication configurations:

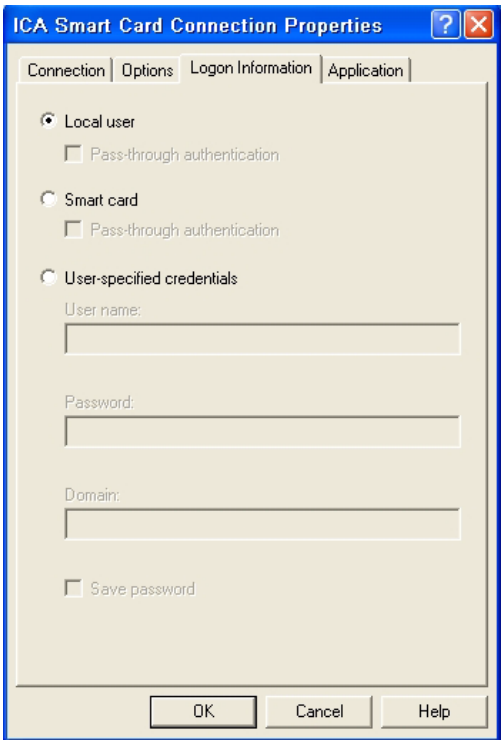
- Local user with pass-through authentication
- Smart card with pass-through authentication

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

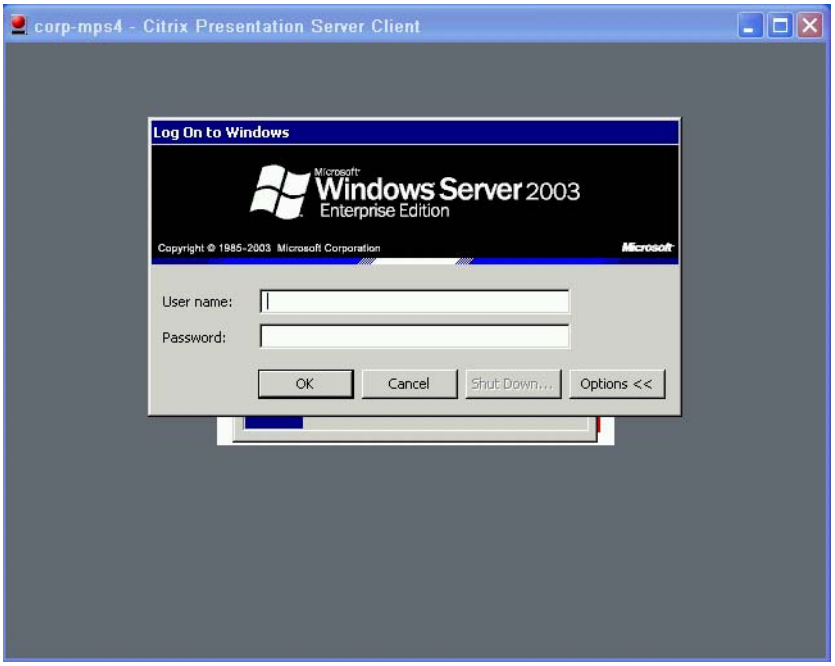
2. Click **Add ICA Connection** to set up a new client connection or to use a pre-existing Citrix connection.



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.



Acronyms

ACM—Adaptive Credential Manager.

CA—Certificate Authority.

CAC—Either Common Access Card (for U.S. government) or Corporate Access Card (for enterprise systems).

CSP—Cryptographic Service Provider.

FIPS—Federal Information Processing Standard.

GP—GlobalPlatform. Replaces OpenPlatform (OP).

PKI—Public Key Infrastructure.

PIV—Personal Identity Verification Card issued by the United States Department of Defense. Displays an expiration date for the card and the card's certificate.

RA—Registration Authority.

SKI—SKI (Symmetric Key Infrastructure) keys are used to encrypt passwords in 2 different modes:

- Synchronous - Generates 1 password without any challenge. The server and the card use the same method to create a password.
- Asynchronous - Encrypts a challenge.

Service and Support

If you would like additional information about ActivClient or other ActivIdentity products, please refer to **http://www.actividentity.com**.

For support issues, you may contact your local ActivIdentity reseller, or ActivIdentity customer support by email at **support@actividentity.com**.

ActivIdentity offices:

ActivIdentity North America

Corporate Headquarters

6623 Dumbarton Circle

Fremont, CA 94555 USA

TEL: +1 (510) 574-0100

FAX: +1 (510) 574-0101

ActivIdentity Europe

European Corporate Headquarters

24-28 Avenue du General de Gaulle

92156 SURESNES, Cedex FRANCE

TEL: +33 (0) 1-42-04-84-00

FAX: +33 (0) 1-42-04-84-84

ActivIdentity Australia

Asia/Pacific Corporate Headquarters

7 Phipps Close

Deakin ACT 2600 AUSTRALIA

TEL: +61-2-62084888

FAX: +61-2-6281-7460

453254-001, 8/2007