Implementation of an ActivCard® smart card solution on HP CCI

This white paper discusses the implementation of ActivCard® smart cards on HP Consolidated Client Infrastructure (CCI). This white paper is not intended as a comprehensive overview of ActivCard smart card technology.

NOTE: The images and instructions in this white paper use Microsoft Windows XPe; however, HP also tested procedures using Microsoft XP Professional and Microsoft Windows CE.NET.

NOTE: The images in this white paper were created using ActivClient™. For information about ActivCard Gold™, see the ActivCard Gold user guide.

Introduction

Smart cards can provide additional security to a CCI implementation. This paper describes a smart card reference implementation that you can use in a dynamic or a static CCI environment.

Prerequisites

This white paper assumes that the reader is familiar with CCI and has a working knowledge of Microsoft Group Policies, Microsoft Certificate Authentication (CA), and setting up smart card readers and middleware.

Reference hardware and software

The following list provides the reference hardware and software used to validate the CCI product with a smart card:

- 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 SP1. 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 t5000 series thin client running Microsoft Windows XPe w/HPSAM blade service installed.
  - HP Compaq t5000 series thin client running Microsoft Windows CE 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 4.28.0.1.
  - 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.
- ActivCard middleware
  - ActivCard ActivClient v5.4.
  - ActivCard Gold v2.2.

Configuration compatibility

HP has tested the following configurations using ActivCard ActivClient v5.4, ActivCard Gold v2.2 and confirmed that the configurations work in a CCI environment.

	HP USB Smart Card Keyboard	**SCM Microsystems SCR331 USB Reader**	**USB Reader SCM Microsystems SCR131 Serial Reader**	**Serial Reader SCM Microsystems SPR337 USB Combo Reader**
HP Thin Client w/XPe	X	X	X	X
HP Thin Client w/CE.net	X	X	X	
HP Desktop w/XP Pro	X	X	X	X

Software configuration

Configure the following items to set up a smart card solution on CCI:

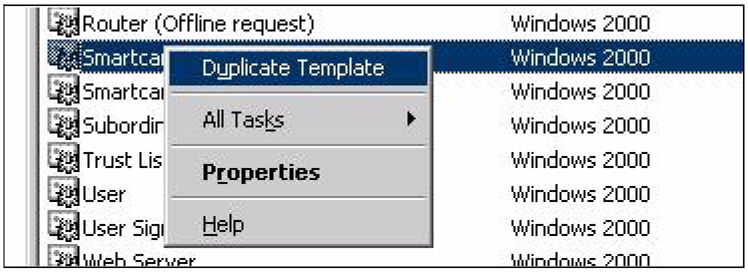
1. Certificate Authentication (CA) service
2. Group policy settings
3. Middleware running on a HP blade PC
4. Smart card client driver

Step 1: Configuring a Certificate Authentication (CA) service

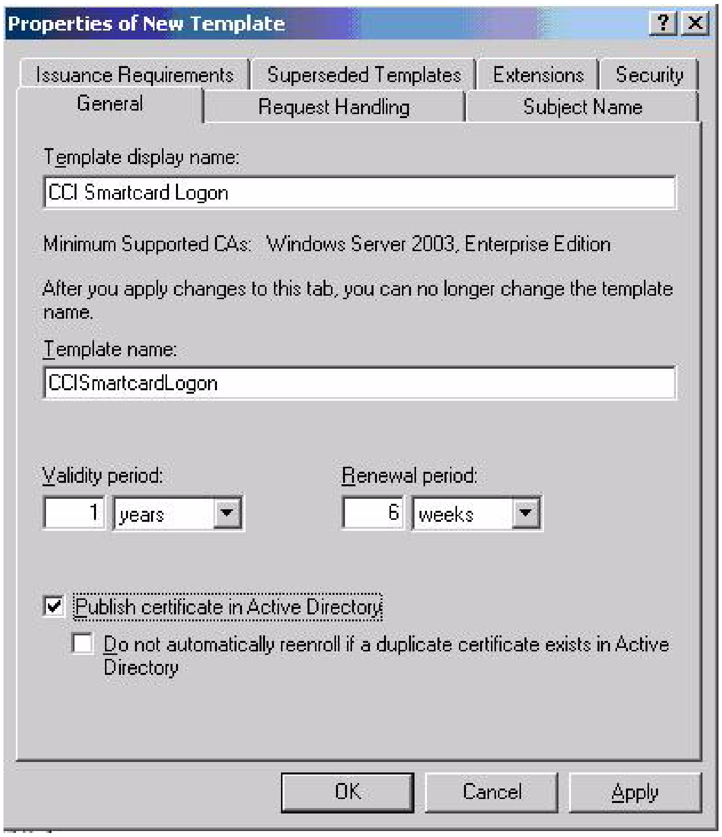
Configure a CA service. This white paper uses Microsoft Certificate Services to configure certificates. Detailed instructions for installing a CA service is beyond the scope of this white paper. For more information about installing Certificate Services, see **http://www.microsoft.com/technet/security/smallbusiness/prodtech/windowsserver2003/build_ent_root_ca.mspx** and **http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00363517/c00363517.pdf**.

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

1. Create an MMC with the following snap-ins:
   - Active Directory Users and Computers
   - Certification Authority
   - Certificate Templates
2. Click **Certificate Templates** and look for the Smartcard Logon certificate 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 Logon`.



Template display name: CCI Smartcard Logon

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name: CCISmartcardLogon

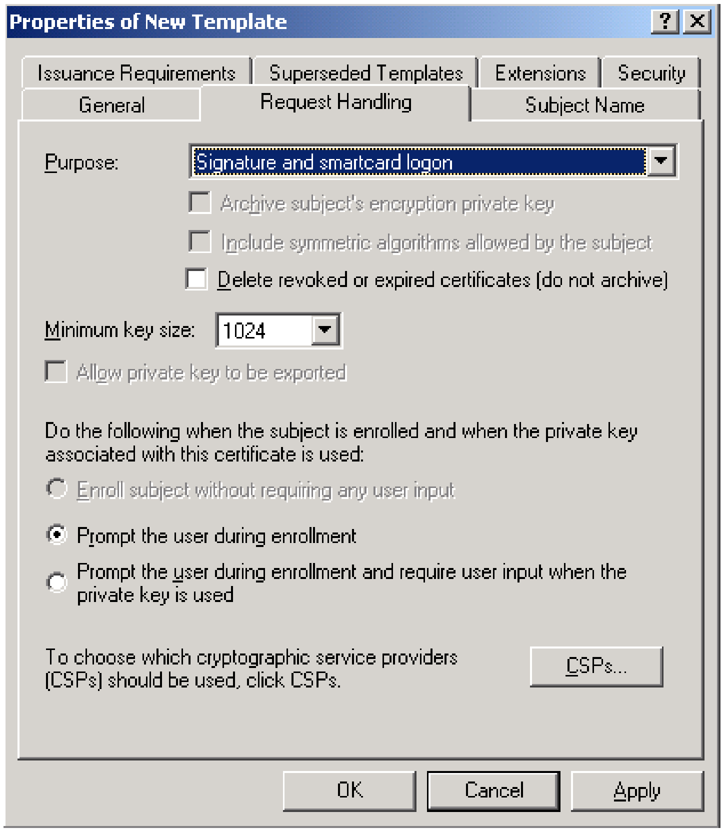
Validity period: 1 years

Renewal period: 6 weeks

☑ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

5. Click the Request Handling tab.



Purpose: Signature and smartcard logon

□ Archive subject's encryption private key

□ Include symmetric algorithms allowed by the subject

□ Delete revoked or expired certificates (do not archive)

Minimum key size: 1024

□ Allow private key to be exported

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

○ Enroll subject without requiring any user input

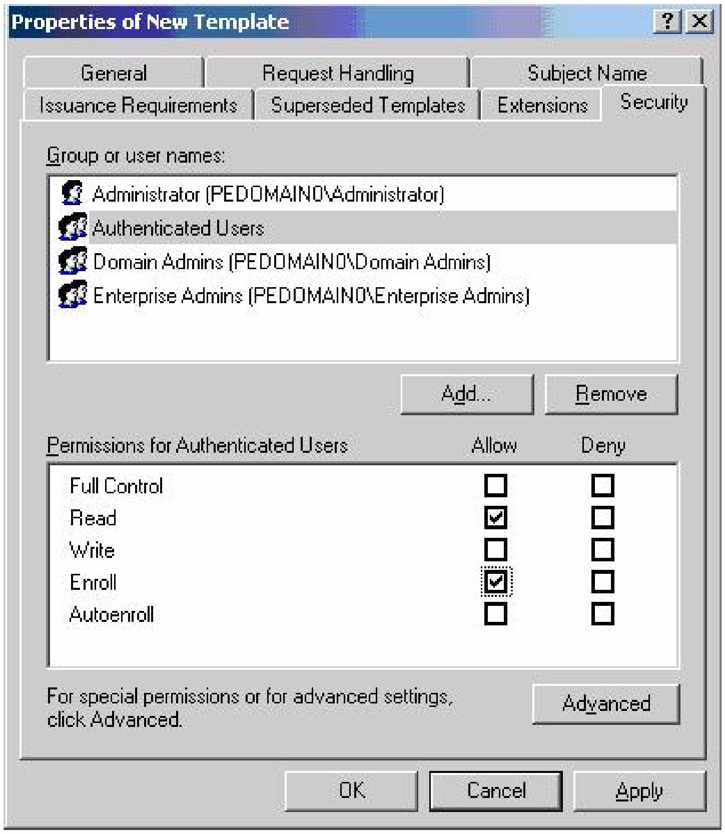
● Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

To choose which cryptographic service providers (CSPs) should be used, click CSPs.

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

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



Group or user names:

- Administrator (PEDOMAIN0\Administrator)
- Authenticated Users
- Domain Admins (PEDOMAIN0\Domain Admins)
- Enterprise Admins (PEDOMAIN0\Enterprise Admins)

Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	□	□

For special permissions or for advanced settings, click Advanced.

You have completed creation of the template.

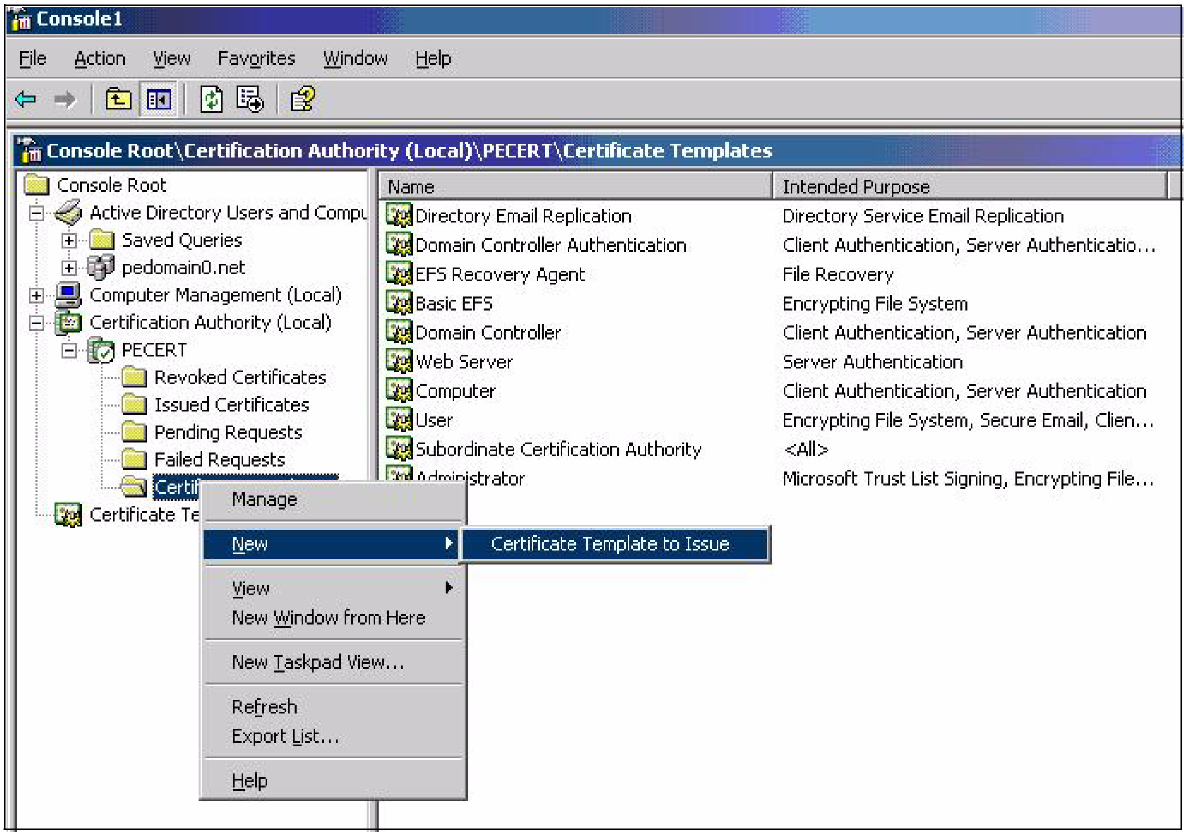
11. Copy the CCI Smartcard Logon certificate template into the Certificate Templates folder under the certificate server.

    a) Expand the Certification Authority object in the MMC you created in step 1.

    b) Expand your CA name.

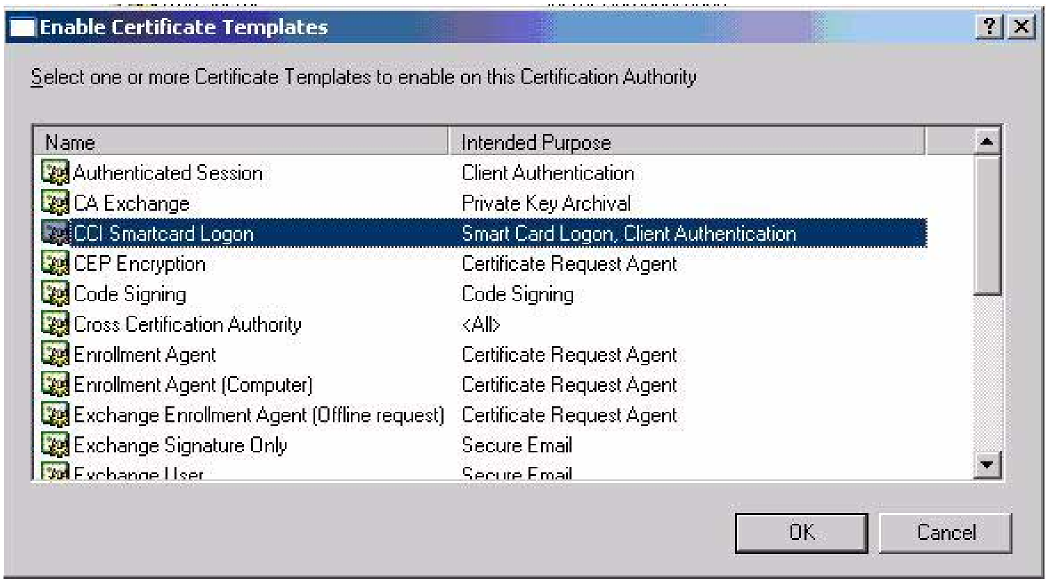
    c) Right-click on the Certificate Templates folder under the CA server.

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


Console1
File Action View Favorites Window Help
Console Root\Certification Authority (Local)\PECERT\Certificate Templates
Console Root
Active Directory Users and Compu
Saved Queries
pedomain0.net
Computer Management (Local)
Certification Authority (Local)
PECERT
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certi
Certificate Te
Manage
New
Certificate Template to Issue
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help

Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authenticatio...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentication
Web Server	Server Authentication
Computer	Client Authentication, Server Authentication
User	Encrypting File System, Secure Email, Clien...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting File...

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



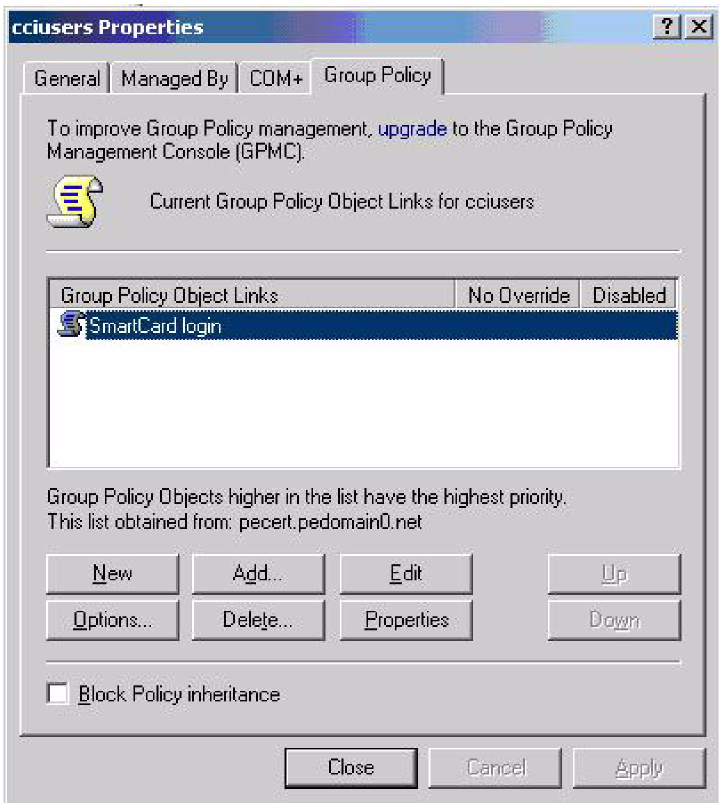
Select one or more Certificate Templates to enable on this Certification Authority

Name	Intended Purpose
Authenticated Session	Client Authentication
CA Exchange	Private Key Archival
CCI Smartcard Logon	Smart Card Logon, Client Authentication
CEP Encryption	Certificate Request Agent
Code Signing	Code Signing
Cross Certification Authority	<All>
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent
Exchange Enrollment Agent (Offline request)	Certificate Request Agent
Exchange Signature Only	Secure Email
Exchange User	Secure Email

Step 2: Group policy setting

Apply the following smart card group policy settings to the computer through a user policy setting or through a computer policy setting:

- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options - Interactive Logon: Require smart card, enable or disable. The default is disabled
- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options - Interactive Logon: Smart card removal behavior, no action or lock workstation or force logoff. The default is no action.



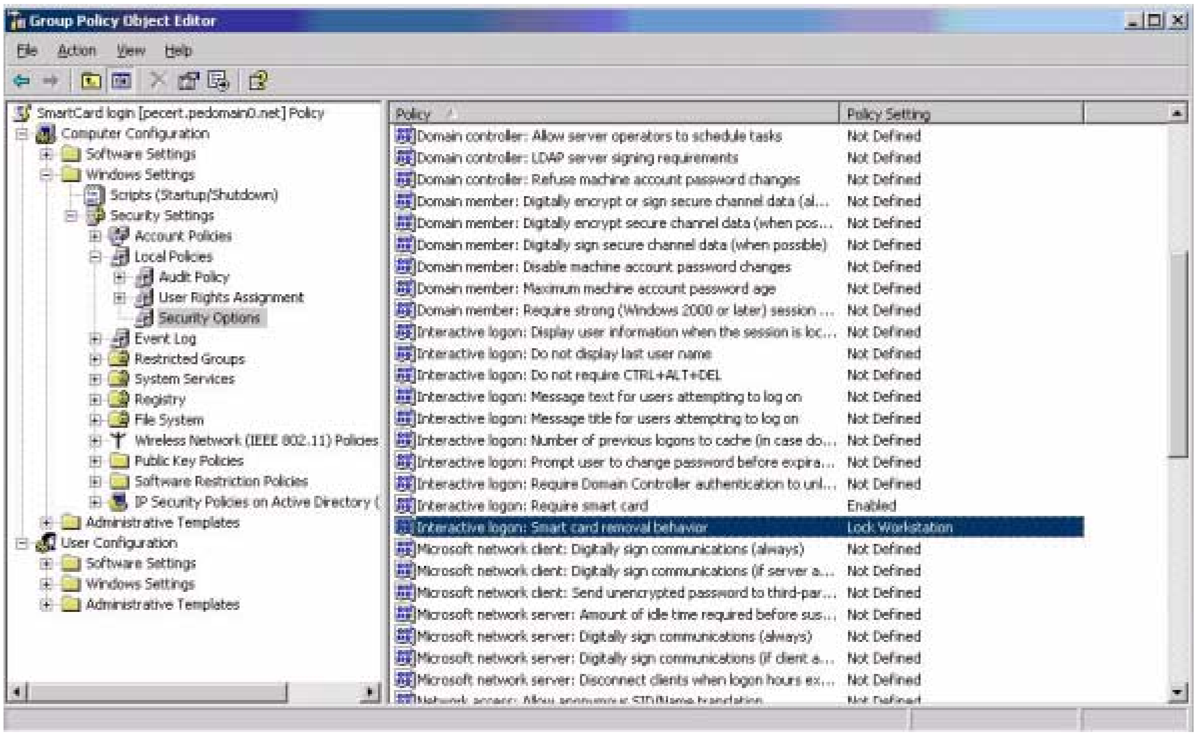
To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).

Current Group Policy Object Links for cciusers

Group Policy Object Links	No Override	Disabled
SmartCard login		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: pecert.pedomain0.net

□ Block Policy inheritance



```
SmartCard login [pecert.pedomain0.net] Policy
  Computer Configuration
    Software Settings
    Windows Settings
      Scripts (Startup/Shutdown)
      Security Settings
        Account Policies
        Local Policies
          Audit Policy
          User Rights Assignment
          Security Options
        Event Log
        Restricted Groups
        System Services
        Registry
        File System
        Wireless Network (IEEE 802.11) Policies
        Public Key Policies
        Software Restriction Policies
        IP Security Policies on Active Directory (
    Administrative Templates
  User Configuration
    Software Settings
    Windows Settings
    Administrative Templates
```

Policy	Policy Setting
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (al...	Not Defined
Domain member: Digitally encrypt secure channel data (when pos...	Not Defined
Domain member: Digitally sign secure channel data (when possible)	Not Defined
Domain member: Disable machine account password changes	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) session ...	Not Defined
Interactive logon: Display user information when the session is loc...	Not Defined
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in case do...	Not Defined
Interactive logon: Prompt user to change password before expira...	Not Defined
Interactive logon: Require Domain Controller authentication to unl...	Not Defined
Interactive logon: Require smart card	Enabled
Interactive logon: Smart card removal behavior	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Not Defined
Microsoft network client: Digitally sign communications (if server a...	Not Defined
Microsoft network client: Send unencrypted password to third-par...	Not Defined
Microsoft network server: Amount of idle time required before sus...	Not Defined
Microsoft network server: Digitally sign communications (always)	Not Defined
Microsoft network server: Digitally sign communications (if client a...	Not Defined
Microsoft network server: Disconnect clients when logon hours ex...	Not Defined
Network access: Allow anonymous SID/Name translation	Not Defined

Step 3: HP blade PC middleware configuration

The following provides HP blade PC software configuration:

- For the purposes of this white paper, an HP CCI implementation with the hardware and software components listed in “Reference hardware and software” on page 2 was used.
- Install one of the following ActivCard middleware packages on the HP Blade PCs:
  - ActivCard ActivClient v5.4
  - ActivCard Gold v2.2

Step 4: Client smart card driver configuration

Configure thin client software (XPe and CE). Detailed instructions for installing drivers on an XPe or CE image is beyond the scope of this white paper. You can find instructions for XPe at **http://h200001.www2.hp.com/bc/docs/support/SupportManual/c00264469/c00264469.pdf** and instructions for CE **http://h200001.www2.hp.com/bc/docs/support/SupportManual/c00234778/c00234778.pdf.**

>> Install the appropriate driver from the list below for the device that you will use.

- HP standard USB Smart Card Keyboard

  Driver: HPKBCCID.sys, version 4.28.0.1

- USB CAC approved smart card reader (SCM Microsystems SCR331 Reader)

  Driver: SCR33X2K.sys, version 4.27.00.01

  NOTE: For Microsoft Windows CE.NET, you may need to copy the drivers from the folder where they were installed (**\Windows**) to the **\Hard Disk\Program Files** folder so the drivers will be written to flash memory.

- Serial CAC approved smart card reader (SCM Microsystems SCR131 Reader)

  NOTE: For Microsoft Windows CE.NET, you may need to copy the drivers from the folder where they were installed (**\Windows**) to the **\Hard Disk\Program Files** folder so the drivers will be written to flash memory.USB Combo Fingerprint & Smart Card Reader (SCM Microsystems SPR337)

  Driver: spr337.sys, version 1.16.00.01

Smart card setup

Initialization of the smart card using Microsoft Remote Desktop Connection

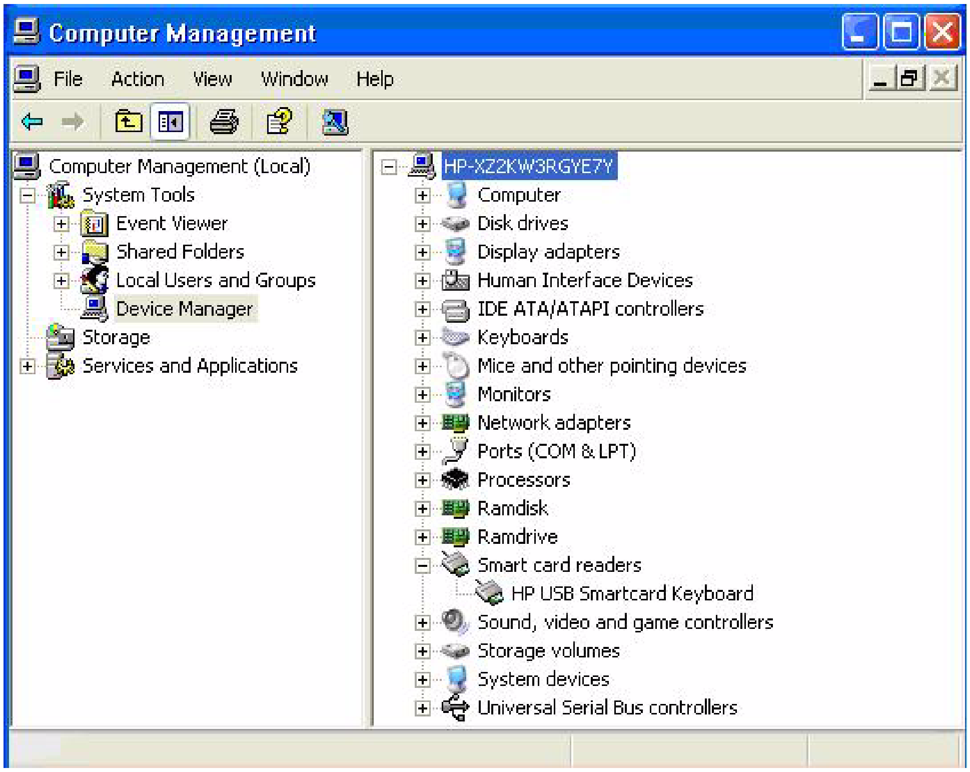
1. Power on the thin client with the smart card reader installed.
2. Open Device Manager to verify that the drivers for the card reader are installed:

   a) Click **Start**.

   b) Right-click on **My Computer** and select **Manage**.

   c) In the left pane, select **Device Manager**.

d) In the right pane, expand **Smart card readers**.



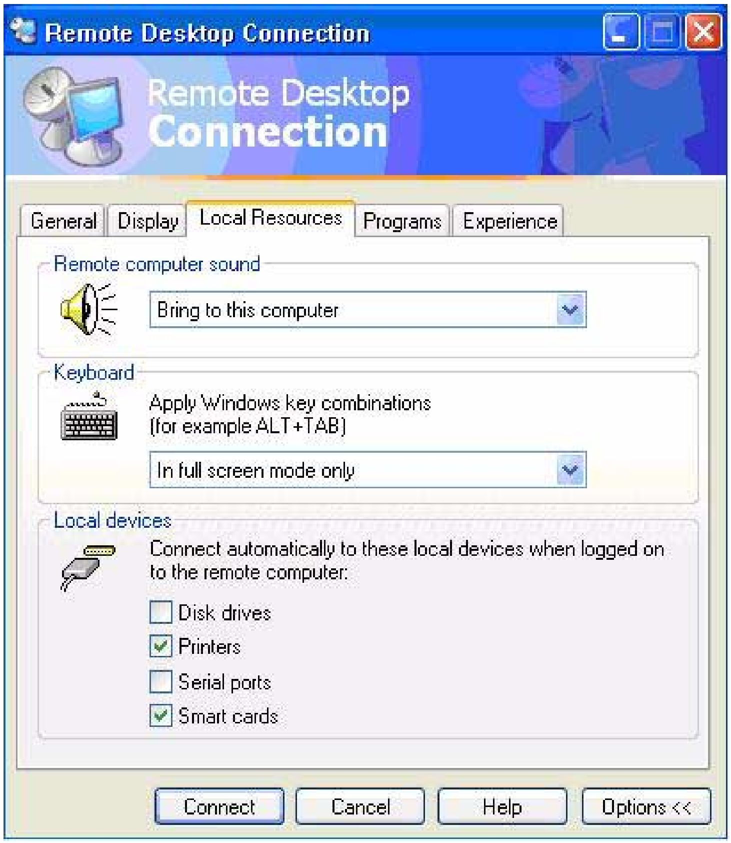
e) Select the installed smart card reader.

f) Under **Device status**, verify the message "This device is working properly."

3. To begin the enrollment from the blade PC side, open the Remote Desktop Connection window by clicking **Start** > **All Programs** > **Accessories** > **Communications**.

4. Select the Local Resources tab.

5. In the **Local Devices** area, select **Smart cards**.



Remote computer sound

Bring to this computer

Keyboard

Apply Windows key combinations
(for example ALT+TAB)

In full screen mode only

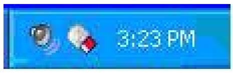
Local devices

Connect automatically to these local devices when logged on to the remote computer:

- ☐ Disk drives
- ☑ Printers
- ☐ Serial ports
- ☑ Smart cards

6. Connect to the blade PC on which you will set up the smart card and log in as a domain-authenticated user.

7. Verify the ActivCard icon is displayed in the system tray.



8. Insert an unprogrammed ActivCard-compatible smart card into the reader. The ActivCard icon in the system tray changes from red to blue.

9. Select the ActivCard icon in the system tray to open the ActivCard utility.

10. Select **Tools** > **New Card** to initialize the smart card.

11. In the **New PIN** and **Verify** boxes, type a PIN for the card, and then click **OK**. The system displays the unlock code for this card in case the PIN is lost.

12. Close the ActivCard utility.

Initialization of the smart card using HP Session Allocation Manager Client (HPSAM Client)

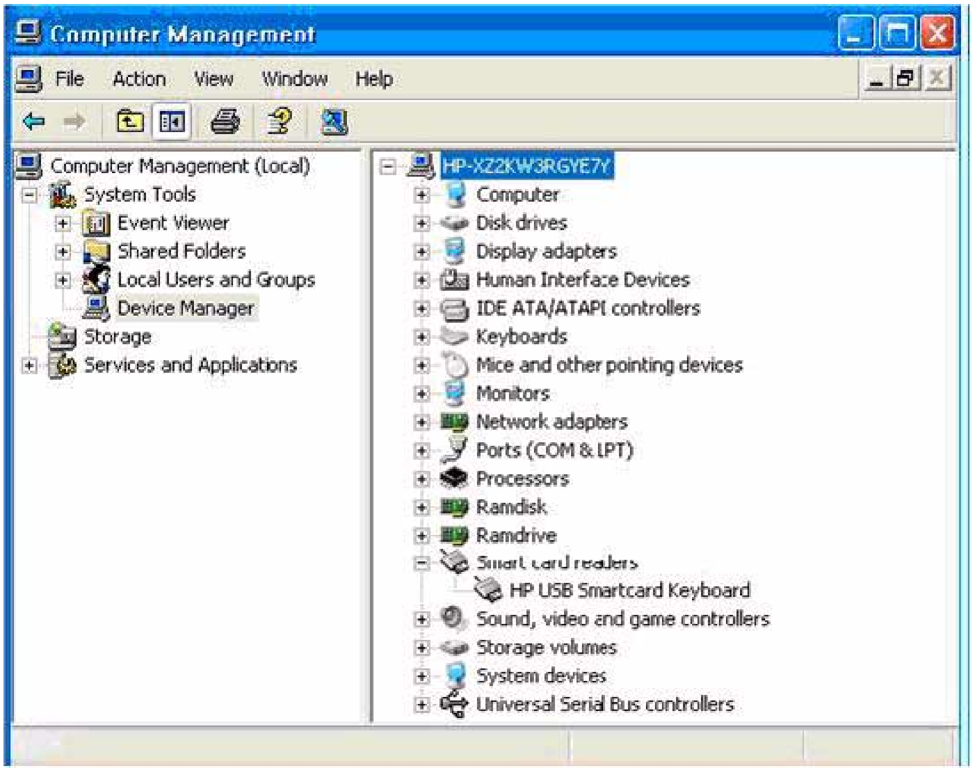
1. Power on the thin client with the smart card reader installed.
2. Open Device Manager to verify that the drivers for the card reader are installed:

   a. Click **Start**.

   b. Right-click on **My Computer** and select **Manage**.

   c. In the left pane, select **Device Manager**.

   d. In the right pane, expand **Smart card readers**.

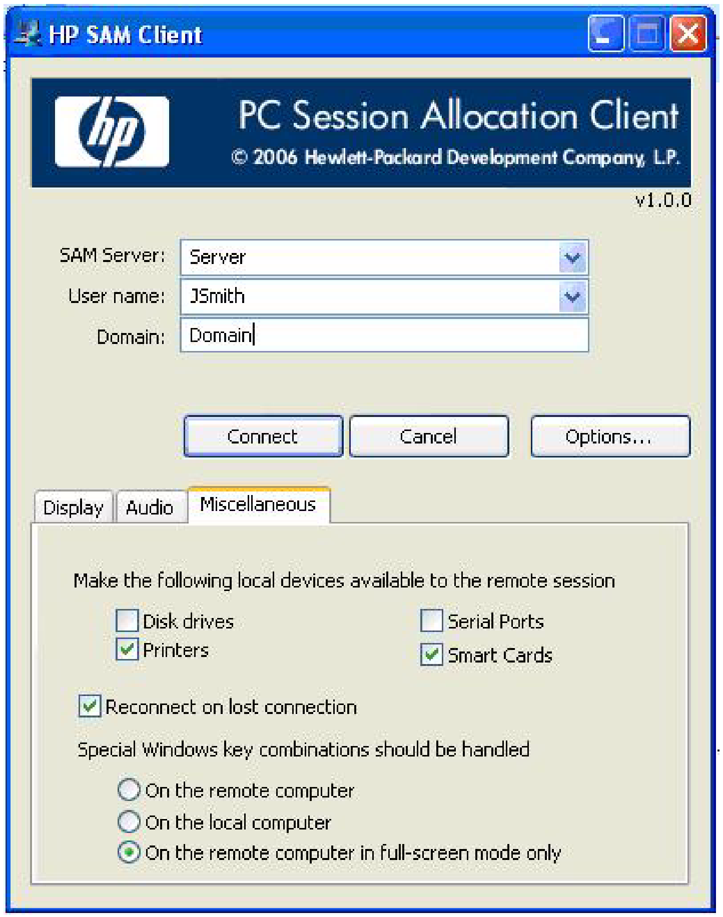


   e. Select the installed smart card reader.

   f. Under Device status, verify the message "This device is working properly."

3. To begin the enrollment from the blade PC side, open the HP PC Session Allocation Client window by clicking **Start** > **All Programs** > **Hewlett-Packard**.
4. Click **Options**.
5. Select the Miscellaneous tab and verify the **Smart Cards** box is selected.

6. Connect to the blade PC on which you will set up the smart card, and then log in as a domain-authenticated user.


HP SAM Client
PC Session Allocation Client
© 2006 Hewlett-Packard Development Company, L.P.
v1.0.0
Connect
Cancel
Options...
Display
Audio
Miscellaneous

SAM Server: Server

User name: JSmith

Domain: Domain

Make the following local devices available to the remote session

☐ Disk drives ☐ Serial Ports

☑ Printers ☑ Smart Cards

☑ Reconnect on lost connection

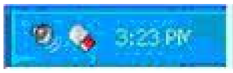
Special Windows key combinations should be handled

○ On the remote computer

○ On the local computer

● On the remote computer in full-screen mode only

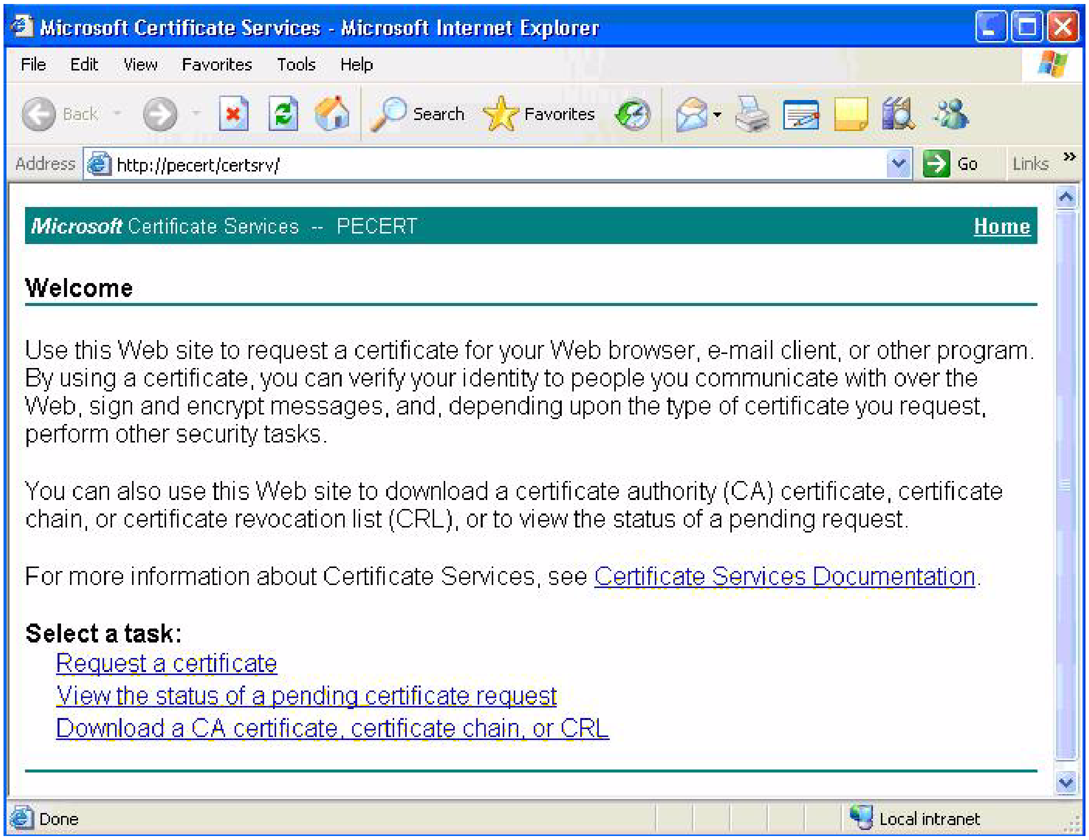
7. Verify the ActivCard icon is displayed in the system tray.



8. Insert an unprogrammed ActivCard-compatible smart card into the reader. The ActivCard icon in the system tray changes from red to blue.
9. Select the ActivCard icon in the system tray to open the ActivCard utility.
10. Select **Tools** > **New Card** to initialize the smart card.
11. In the **New Pin** and **Verify** boxes, type a PIN for the card, and then click **OK**. The system displays the unlock code for this card in case the PIN is lost.
12. Close the ActivCard utility.

Requesting a certificate from the blade PC

1. Open Internet Explorer and go to the Certification Server enrollment Web site. The address of this Web site was determined when the Certification Server was set up (see “Step 1: Configuring a Certificate Authentication (CA) service” on page 4). If you do not know the Web address, consult your network administrator. In this example, the address used is **http://pecert/certsrv**.
2. Click the **Request a Certificate** task.



Microsoft Certificate Services -- PECERT **Home**

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

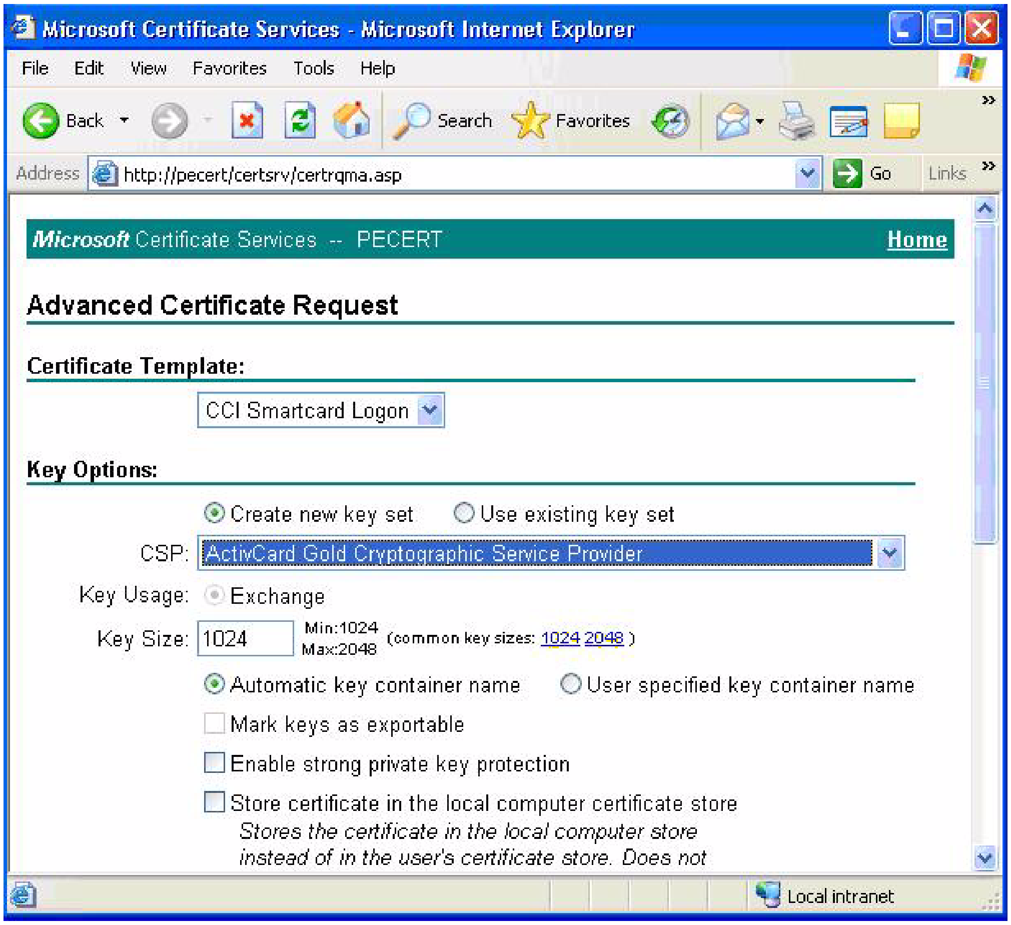
Select a task:
- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL

3. On the Request a Certificate page, click **advanced certificate request**.
4. On the Advanced Certificate Request page, select **Create and submit a request to this CA**.
5. On the Advance Certificate Request page:

   a) Select **CCI Smartcard Logon** as the certificate template.

   b) Select **ActivCard Gold Cryptographic Service Provider** as the CSP.

   c) Submit the request, which requests a CCI SmartCard Logon certificate for the selected user.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Local intranet

Address: http://pecert/certsrv/certrqma.asp

Microsoft Certificate Services -- PECERT **Home**

Advanced Certificate Request

Certificate Template:

CCI Smartcard Logon

Key Options:

● Create new key set ○ Use existing key set

CSP: ActivCard Gold Cryptographic Service Provider

Key Usage: ● Exchange

Key Size: 1024 Min:1024 Max:2048 (common key sizes: 1024 2048)

● Automatic key container name ○ User specified key container name

□ Mark keys as exportable

□ Enable strong private key protection

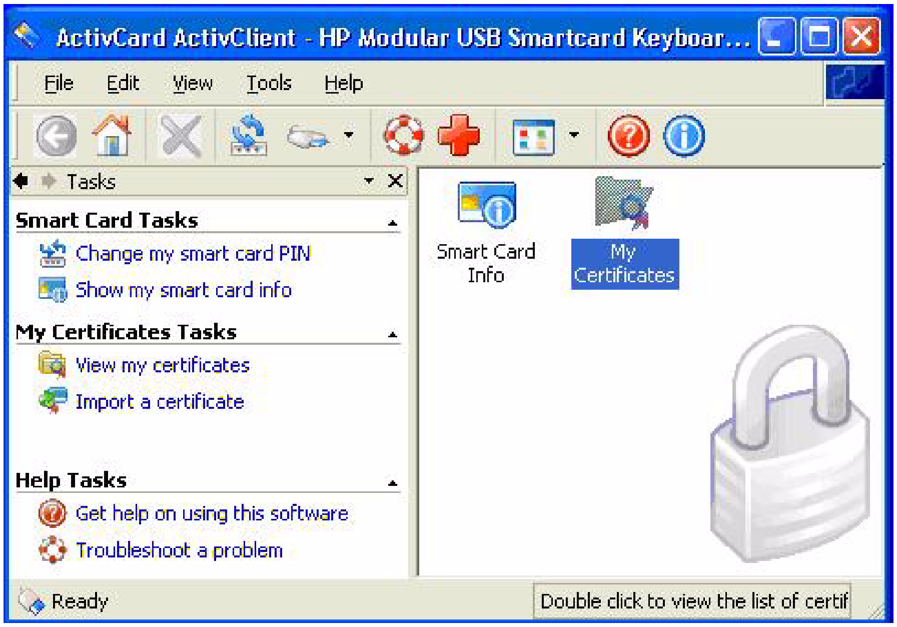
□ Store certificate in the local computer certificate store

Stores the certificate in the local computer store instead of in the user's certificate store. Does not

6. If a warning message displays about a potential scripting violation, press **Yes** to continue with the certificate request.
7. After the system generates the public and private keys, the page to install the certificate displays. Select **Install this certificate**. This command installs the users's certificate onto the smart card.
8. If a warning message displays about a potential scripting violation, press **Yes** to continue with the certificate request.
9. Upon successful completion, the system displays the Certificate installed page. You may close Internet Explorer.

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 ActivCard Gold utility.
2. In the right pane, select the **My Certificates** icon. The system displays the username ID.



Ready

Double click to view the list of certif

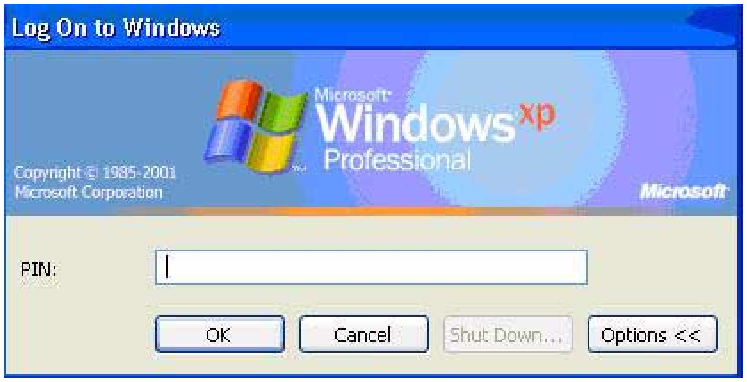
3. Select the username ID to view the installed certificate, which shows:
   - who it was issued to
   - who it was issued by
   - valid dates

Usage cases

Usage case 1: User authentication from client device to blade PC 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.



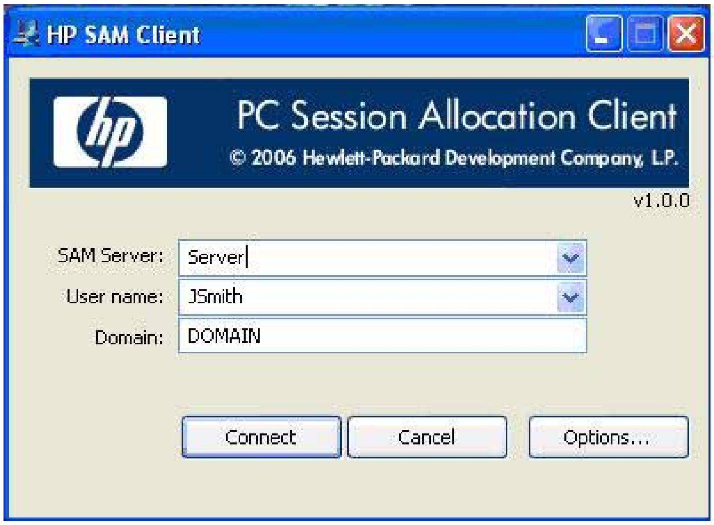
4. Type the PIN that you assigned. The user is logged into the blade

Usage case 2: User authentication from client device to blade PC 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.


HP SAM Client

PC Session Allocation Client

© 2006 Hewlett-Packard Development Company, L.P.

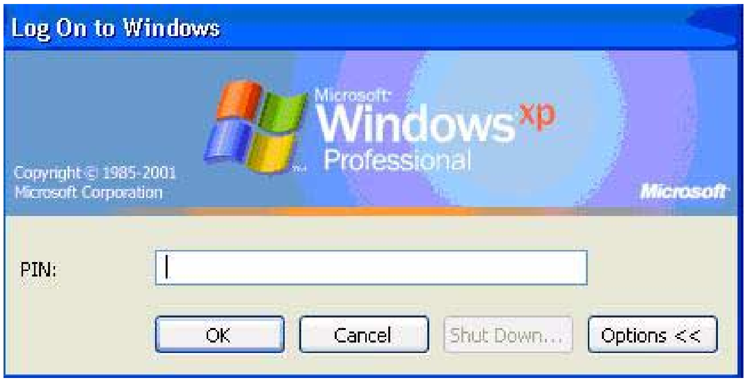
v1.0.0

SAM Server: Server

User name: JSmith

Domain: DOMAIN

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

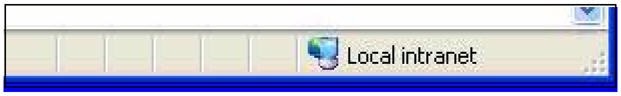

Log On to Windows

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

Usage case 3: Accessing secure Web site

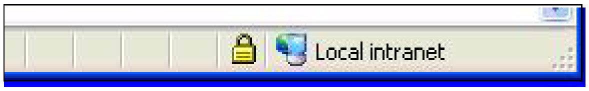
The following steps provide instructions for accessing a secure Web site using an ActivCard through a blade PC. Installing and configuring a secure Web site is beyond the scope of this white paper; therefore, the white paper assumes the secure Web site is already functional and accessible from the blade PC. 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 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**.

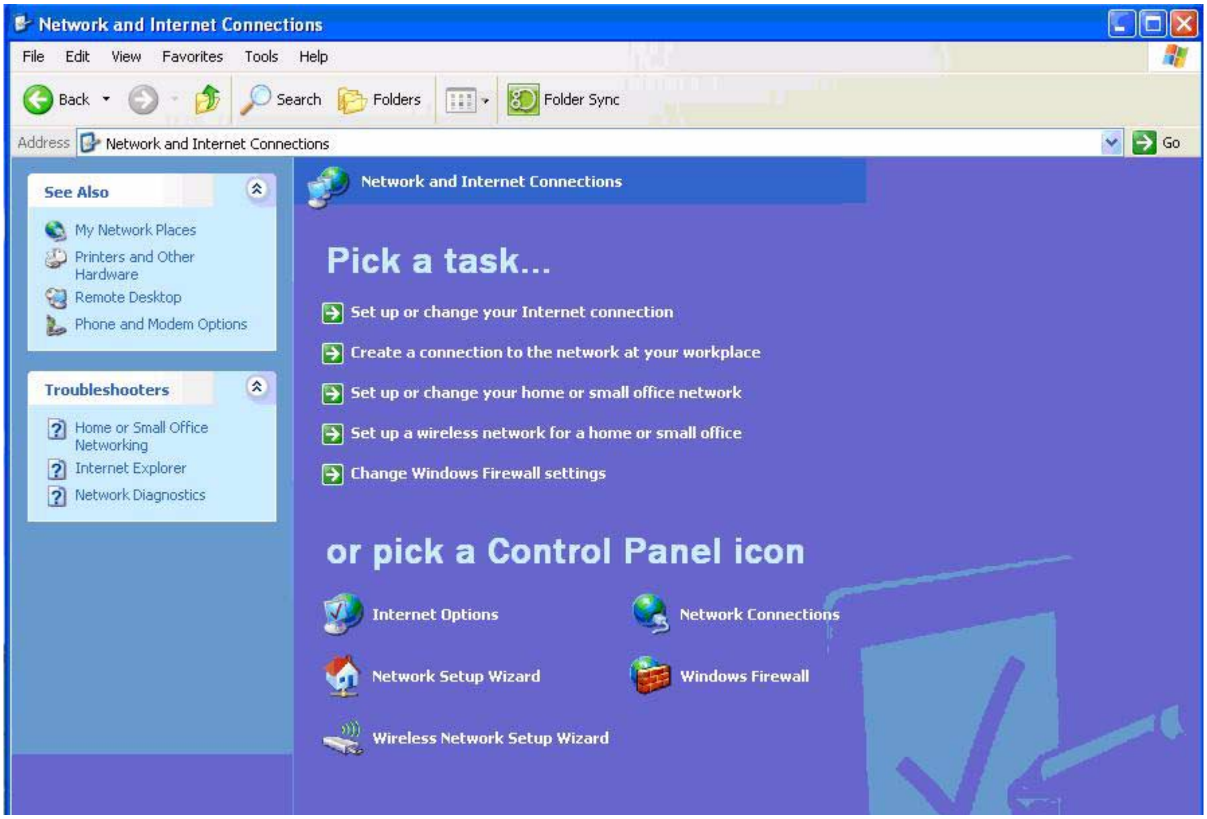
   The LED on the card reader indicates when the Web site is accessing the smart card to verify whether the certificate is approved for the site.
6. After the secure Web site displays, a lock icon in the lower right corner of Internet Explorer confirms that you are connected to a secure Web site.



Usage case 4: User authentication using VPN through firewall to blade PC

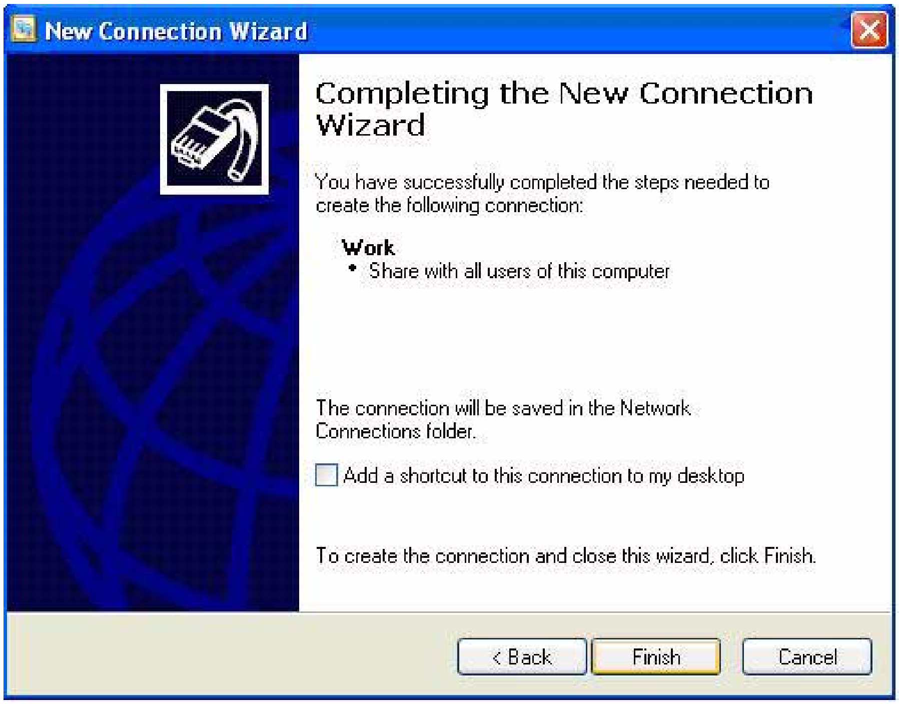
Instructions for installing and configuring a VPN tunnel with a firewall is beyond the scope of this white paper; therefore, the white paper assumes the VPN tunnel and firewall are already installed and functional. The white paper also assumes that you have a broadband Internet connection and that ActivCard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


Network and Internet Connections
File
Edit
View
Favorites
Tools
Help
Back
Search
Folders
Folder Sync
Address
Network and Internet Connections
Go
See Also
My Network Places
Printers and Other Hardware
Remote Desktop
Phone and Modem Options
Troubleshooters
Home or Small Office Networking
Internet Explorer
Network Diagnostics
Network and Internet Connections
Pick a task...
Set up or change your Internet connection
Create a connection to the network at your workplace
Set up or change your home or small office network
Set up a wireless network for a home or small office
Change Windows Firewall settings
or pick a Control Panel icon
Internet Options
Network Connections
Network Setup Wizard
Windows Firewall
Wireless Network Setup Wizard

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**.



Completing the New Connection Wizard

You have successfully completed the steps needed to create the following connection:

Work

- Share with all users of this computer

The connection will be saved in the Network Connections folder.

□ Add a shortcut to this connection to my desktop

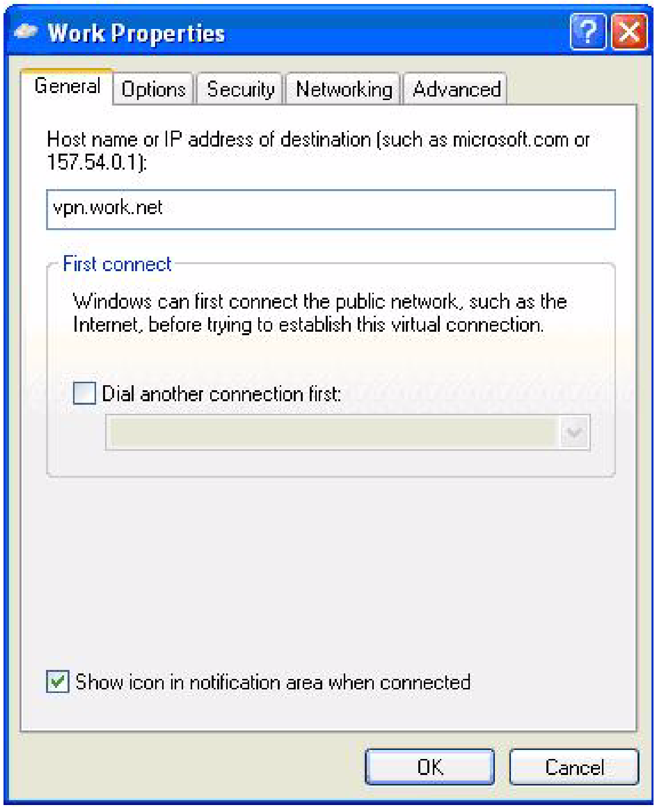
To create the connection and close this wizard, click Finish.

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**.



Host name or IP address of destination (such as microsoft.com or 157.54.0.1):

vpn.work.net

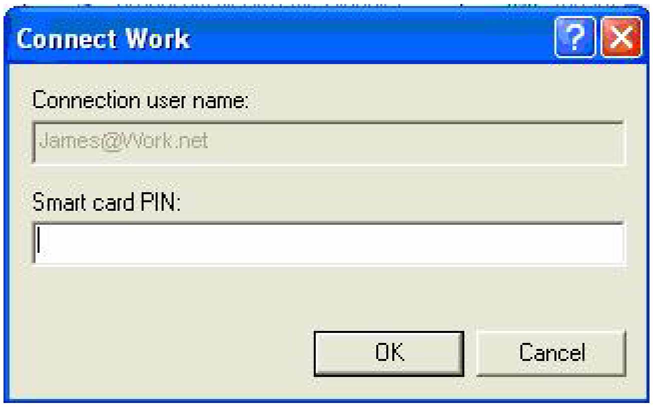
Windows can first connect the public network, such as the Internet, before trying to establish this virtual connection.

□ Dial another connection first:

☑ Show icon in notification area when connected

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**.



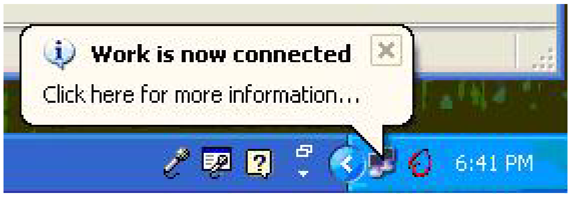
Connection user name:

James@Work.net

Smart card PIN:

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.



Work is now connected

Click here for more information...

Additional information

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 ActivCard, see **http://www.activcard.com.**

409531-002, 4/2006