Implementation of an ActivCard $\ensuremath{\mathbb{R}}$ smart card solution on HP CCI

hp

Introduction
Prerequisites
Reference hardware and software
Configuration compatibility
Software configuration
Step 1: Configuring a Certificate Authentication (CA) service
Step 2: Group policy setting9
Step 3: HP blade PC middleware configuration
Step 4: Client smart card driver configuration
Smart card setup
Initialization of the smart card using Microsoft Remote Desktop Connection
Initialization of the smart card using HP Session Allocation Manager Client (HPSAM Client) . 14
Requesting a certificate from the blade PC16
Usage cases
Usage case 1: User authentication from client device to blade PC using RDP
Usage case 2: User authentication from client device to blade PC using HPSAM client 19
Usage case 3: Accessing secure Web site
Usage case 4: User authentication using VPN through firewall to blade PC
Additional information



1

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	Х	Х	Х	Х
HP Thin Client w/CE.net	Х	Х	Х	
HP Desktop w/XP Pro	Х	Х	Х	Х



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/smallbusi-ness/prodtech/windowsserver2003/build_ent_root_ca.mspx and http://h20000.www2.hp.com/bc/docs/support/Suppor

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**.

Router (Ol	fline request)	Windows 2000
Con Smartcar	Duplicate Template	Windows 2000
Smartcar		Windows 2000
Subordin	All Tas <u>k</u> s 🔹 🕨	Windows 2000
Trust Lis	Properties	Windows 2000
User -	Topercies	Windows 2000
User Sigi	Help	Windows 2000
Web Serve	ər	Windows 2000



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

operties of New Template		?
Issuance Requirements Superseded Templates General Request Handling	Extensions Subject N	Security Name
Template display name: CCI Smartcard Logon		
Minimum Supported CAs: Windows Server 2003, E After you apply changes to this tab, you can no long name	nterprise Editio ger change the	n template
Iemplate name:		
CCISmartcardLogon		
Validity period: <u>B</u> enewal period 1 years ▼ 6 weeks	•	
Publish certificate in Active Directory		
 Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificatory 	ertificate exists i	in Active



5. Click the Request Handling tab.

Properties of New 1	remplate	<u>? ×</u>
Issuance Requirem General	ents Superseded Templates Request Handling	Extensions Security Subject Name
Purpose: ∬ Γ Γ	Signature and smartcard logon Archive subject's encryption pr Include symmetric algorithms a Delete revoked or expired certi	ivate key flowed by the subject ficates (do not archive)
Minimum key size: Allow private k Do the following w associated with th Enroll subject of	1024 ey to be exported hen the subject is enrolled and w is certificate is used: without requiring any user input	hen the private key
 Prompt the use Prompt the use private key is to To choose which (CSPs) should be to (CSPs) 	er during enrollment er during enrollment and require us used cryptographic service providers used, click CSPs.	ser input when the
	ок с	ancel <u>A</u> pply

- 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.

General Request Handling Subject Name ance Requirements Superseded Templates Extensions Security up or user names: Administrator (PEDOMAIN0\Administrator) Administrator (PEDOMAIN0\Domain Admins) Authenticated Users Domain Admins (PEDOMAIN0\Domain Admins) Enterprise Admins (PEDOMAIN0\Enterprise Admins) Enterprise Admins (PEDOMAIN0\Enterprise Admins)	perties of New Template			?
ance Requirements Superseded Templates Extensions Security up or user names: Administrator (PEDOMAINO\Administrator) Authenticated Users Domain Admins (PEDOMAINO\Domain Admins) Enterprise Admins (PEDOMAINO\Enterprise Admins) Enterprise Admins (PEDOMAINO\Enterprise Admins)	General Request Handli	ing	Subjec	ct Name
up or user names: Administrator (PEDOMAIN0\Administrator) Authenticated Users Domain Admins (PEDOMAIN0\Domain Admins) Enterprise Admins (PEDOMAIN0\Enterprise Admins) Enterprise Admins (PEDOMAIN0\Enterprise Admins)	ssuance Requirements Superseded T	emplates 📔	Extension	s Securit
Administrator (PEDOMAIN0\Administrator) Authenticated Users Domain Admins (PEDOMAIN0\Domain Admins) Enterprise Admins (PEDOMAIN0\Enterprise Admins) Add Add Bemove Missions for Authenticated Users Allow Deny Ull Control Head Vite Inroll Inrol	Group or user names:			
Authenticated Users Domain Admins (PEDOMAIN0\Domain Admins) Enterprise Admins (PEDOMAIN0\Enterprise Admins) Add Add Add Bemove missions for Authenticated Users Allow Deny ull Control lead Vrite Inroll Inroll Inroll	🛃 Administrator (PEDOMAINO\Adminis	strator)		
Domain Admins (PEDOMAIN0\Domain Admins) Enterprise Admins (PEDOMAIN0\Enterprise Admins) Add Remove Add Remove missions for Authenticated Users Allow Deny 'ull Control I Pead I Vrite I Control I Incoll I	👧 Authenticated Users			
Enterprise Admins (PEDOMAIN0\Enterprise Admins) Add Remove missions for Authenticated Users Allow Deny 'ull Control Image: Control Image: Control Image: Control Yrite Image: Control Image: Control Image: Control Image: Control Yrite Image: Control Image: C	🕵 Domain Admins (PEDOMAINO\Dom	ain Admins)		
Add Remove missions for Authenticated Users Allow Deny 'ull Control Image: Control Con	REINTERPRISE Admins (PEDOMAINO\Er	nterprise Adm	iins)	
Add <u>Remove</u> missions for Authenticated Users Allow Deny full Control Image: Control C	2700 C	14	10	
Add Remove missions for Authenticated Users Allow Deny full Control Image: Control Contron Control Control Control Control Con				
Aga Hemove missions for Authenticated Users Allow Deny full Control Image: Control Con				
missions for Authenticated Users Allow Deny full Control Image: Control Image: Control Read Image: Control Image: Control Vrite Image: Control Image: Control Control Image: Control Image: Control Control Image: Control Image: Control Control Image: Control Image: Control		. د. ه	1	I
Full Control Image: Control Control Read Image: Control		A <u>d</u> d	<u>I</u>	<u>R</u> emove
Read ☑ □ Vrite □ □ inroll ☑ □ sutoenroll □ □	Permissions for Authenticated Users	Add Allo	<u>I</u>	<u>R</u> emove Deny
Vrite Crroll	Permissions for Authenticated Users Full Control	A <u>d</u> d Alla	<u>]</u> w	<u>R</u> emove
inroll 🗹 🗖	Permissions for Authenticated Users Full Control Read	Add Alla	<u> </u> w]]]	Bemove
Sutoenroll	<u>P</u> ermissions for Authenticated Users Full Control Read Write	Add Allo	<u>I</u> >w]]]	Bemove
	Permissions for Authenticated Users Full Control Read Write Enroll		 >wv]]]]]	Bemove
	Permissions for Authenticated Users Full Control Read Write Enroll Autoenroll		<u> </u> ww 0 0 0 0 0 0 0	Bemove
	Permissions for Authenticated Users Full Control Read Write Escoll	Add Alla	 >>>>]]]]	Bemove
	Permissions for Authenticated Users Full Control Read Write Enroll Autoenroll			Bemove
special permissions or for advanced settings, Advanced	Permissions for Authenticated Users Full Control Read Write Enroll Autoenroll	Add Alla E E ettings,		Bemove Deny Deny Dury Dury Dury Dury Dury Dury Dury Dur
special permissions or for advanced settings, <u>Advanced</u>	Permissions for Authenticated Users Full Control Read Write Enroll Autoenroll For special permissions or for advanced s click Advanced.	Add Alle E E ettings,		Bemove Deny Deny dyanced
special permissions or for advanced settings, Advanced	Permissions for Authenticated Users Full Control Read Write Enroll Autoenroll For special permissions or for advanced s click Advanced.	Add Alla E ettings,		<u>R</u> emove Deny Deny Deny dyanced

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.

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

Name	Intended Purpose	A
🙀 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></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	_
Sol 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.

o improve Grou	up Policy manage	ment, upgrade to th	ne Group Po	blicy
Aanagement Co	onsole (GPMC).			
式 Curi	rent Group Policy	Object Links for cc	iusers	
C D L C		-NL	Quarrida	D' LL I
SmartCard	Joject Links login	Ni	est prioritu	Uisabled
Group Policy C SmartCard Group Policy Ob This list obtained	Joject Links login jects higher in the d from: pecert.pec	e list have the highe Iomain0.net	est priority.	
aroup Policy C SmartCard iroup Policy Ob his list obtained <u>N</u> ew	Joject Links login jects higher in the d from: pecert.pec	e list have the highe Jomain0.net	est priority.	
iroup Policy 0 SmartCard iroup Policy 0t his list obtained <u>N</u> ew <u>O</u> ptions	Joject Links login jects higher in the d from: pecert.pec Add Dele <u>t</u> e	e list have the highe lomain0.net <u>E</u> dit <u>P</u> roperties	est priority.	Uisabled Up Do <u>w</u> n
Group Policy C SmartCard Group Policy Ob This list obtained	Joject Links login jects higher in the d from: pecert.pec	e list have the highe	est priority.	Disable



in Group Policy Object Editor			- D X
Ele Action View Help			
SmartCard login [pecert.pedcmsin0.net] Pokcy Software Settings Software Settings Sortists (Startup(Shutdown)) Security Software Local Pokces Software Settings Software Settings Software Settings Software Settings System Services System Services System Services Software Settings Software Setings Software Settings Software Settings Software Sett	Policy ////////////////////////////////////	Policy Setting Not Defined	
	Microsoft network server: Digitally sign communications (if client a Microsoft network server: Disconnect clients when logon hours ex Microsoft network server: Also anonymy of Sthillama transition	Not Defined Not Defined 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/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 DiskProgram 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.

🕲 Rema	ote Desktop Connection
E	Remote Desktop Connection
General	Display Local Resources Programs Experience
Remo	te computer sound
Keybo	ard Apply Windows key combinations (for example ALT+TAB)
	In full screen mode only
Local	devices
P	 Connect automatically to these local devices when logged on to the remote computer:
1.1	Disk drives
	Printers
	Serial ports
	Smart cards
	Connect Cancel Help Options <<

- 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.

🧐 🍫 3:23 PM

- 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 domainauthenticated user.

💐 HP SAM Clie	ent 🔚 🗖 🔀
Ø	PC Session Allocation Client © 2006 Hewlett-Packard Development Company, L.P. v1.0.0
SAM Server:	Server
User name:	JSmith
Domain:	Domain
Display Audio Make the fo Disk Prin Reconne Special Winu On On On	Miscellaneous Miscel

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

🧐, 💊 3:23 PM

- 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

- 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 - Microsoft Internet Explorer 🗧	
File Edit View Favorites Tools Help	1
🕞 Back - 🐑 - 💌 🗟 🏠 🔎 Search 📌 Favorites 🚱 🔗 🍚 🕞 🛄 🎇 🦓	
Address 🕘 http://pecert/certsrv/	Links »
	^
Microsoft Certificate Services PECERT Ho	ome
Welcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other progra 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 <u>Certificate Services Documentation</u> .	am. ∋ ≡
Select a task:	
Request a certificate	
View the status of a pending certificate request	
Download a CA certificate, certificate chain, or CRL	
	~
🕘 Done 😔 Local intranet	

- 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 Ex	plorer 🔲 🗖 🔀
File Edit View Favorites Tools Help	
🚱 Back 🔹 🕥 - 💌 🗟 🏠 🔎 Search 📌 Fa	vorites 🚱 🎯 🎽 🔛 🎽
Address 🕘 http://pecert/certsrv/certrgma.asp	Go Links 🎽
Microsoft Certificate Services PECERT Advanced Certificate Request	Home
Certificate Template:	
CCI Smartcard Logon 😪	
Key Options:	
💿 Create new key set 🛛 🔿 Use exist	ng key set
CSP: ActivCard Gold Cryptographic Service F	Provider 💌
Key Usage: 💿 Exchange	
Key Size: 1024 Min:1024 Max:2048 (common key sizes: 102:	1 2048)
O Automatic key container name	User specified key container name
Mark keys as exportable	a and a second definition of the second s
Enable strong private key protection	
Store certificate in the local compute Stores the certificate in the local co instead of in the user's certificate s	er certificate store omputer store tore. Does not
ê	S Local intranet

- 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.

🔦 ActivCard ActivClient - HP Mod	ular USB Smartcard Keyboar 🔳 🗖 🔀
Eile Edit Yiew Iools Help	1
) G 🚹 🗙 🏩 🏎 🔇	🤅 🖶 🔃 - 🥝 🕕
🕈 🕸 Tasks 🛛 👻 🗙	
Smart Card Tasks	
🕍 Change my smart card PIN	Smart Card My
5 Show my smart card info	Info Certificates
My Certificates Tasks	
View my certificates	
Tradeuk a saukičinska	16
Import a certificate	
1.3 Telefo	9
Help Tasks	
@ Get help on using this software	
🛟 Troubleshoot a problem	
🔖 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.

Log On t	o Windows	4
Copyright @ Microsoft Cor	1985-2001 rporation	Microsoft
PIN:	OK Cancel Shut Down Opti	ons <<

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.

(p)	PC Session Allocation © 2006 Hewlett-Packard Development Co	Clier
		۷1.
SAM Server:	Server	1
User name:	JSmith 🗸	
Domainu	DOMAIN	1

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

Log On t	o Windows	
Copyright © Microsoft Co	1985-2001 rporation	Microsoft
PIN:	OK Cancel Shut Down	Options <<

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.



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.

New Connection Wizard	1 🛛
	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.
	< Back Finish Cancel

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.

Work	Propert	ies		
eneral	Uptions	Security	Networking	Advanced
Host na 157.54.	ame or IP a 0.1):	address of	destination (su	ch as microsoft.co
vpn.wo	ork.net			
First o	onnect			
Wine Inter	dows can net, befor	first conne e trying to (ect the public n establish this v	etwork, such as th irtual connection.
)ial anothe	er connecti	ion first:	arienarien
1				
🗹 Sho	w icon in r	notification	area when co	nnected
			(

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.

Connect Work		? 🔀
Connection user name:		
James@Work.net		
Smart card PIN:		
	OK	Cancel

While establishing the VPN connection, the system displays <code>Verifying username and password and Authenticated</code>.



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



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.

Microsoft, MS-DOS, Windows, and Windows NT are trademarks of Microsoft Corporation in the U.S. and other countries. 409531-002, 4/2006



^{© 2006} 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.

Free Manuals Download Website <u>http://myh66.com</u> <u>http://usermanuals.us</u> <u>http://www.somanuals.com</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.com</u> <u>http://www.404manual.com</u> <u>http://www.luxmanual.com</u> <u>http://aubethermostatmanual.com</u> Golf course search by state

http://golfingnear.com Email search by domain

http://emailbydomain.com Auto manuals search

http://auto.somanuals.com TV manuals search

http://tv.somanuals.com