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



Introduction
Prerequisites
Reference hardware and software
Reference Documents
Installing GemSafe Libraries 5.0 SE to Server and Client PCs (Optional)5
Installing Microsoft Certificate Services9
Configuring a Certificate Authority (CA) service
Configuring Microsoft Certificate Authority to Issue Smart Card User Certificate
Manually issue Smart Card User Certificate
Testing the Smart Card
Creating Customized User Install Packages for Clients PCs (Optional)
Additional Information
Using a Smart Card For Windows Network Login
Administration of the GemSafe Smart Card
Working with GemSafe Libraries
Usage cases
Usage case 1: User authentication from blade PC to Active Directory Domain
Usage case 2: User authentication from client device to blade PC or
Active Directory Server using RDP
Usage case 3: User authentication from client device to blade PC or Active Directory Server using HPSAM client
Usage case 4: Accessing secure Web site
Usage case 5: User authentication using VPN through firewall to blade PC or
Active Directory Server
Usage case 6: User authentication from client device using Citrix server
Service and Support



Introduction

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

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

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 Replacing the outdated and easy to hack "user name and password" authentication method, corporate employees can log onto corporate recourses via HP thin clients using the Gemalto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

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

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

Prerequisites

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



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

b. Install your reader driver.

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

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

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

Reference hardware and software

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

- Load Balancer
 - HP Server running F5 networks BigIP version 4.6.4.

or

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



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

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

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

Reference Documents

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

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



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

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

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

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

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

Choose 9	ietup Language	×
2	Select the language for this installation from the choices below).
	English (United States)	
	OK Cancel	



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

🙀 GemSafe Standard Edition 5	5.0 Administrator - InstallShield Wizard	x
	Welcome to the InstallShield Wizard for GemSafe Standard Edition 5.0 Administrator	
	< Back Next > Cancel	

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

🙀 GemSafe Standard Edition 5.0 Admi	inistrator - Inst	allShield Wizard	×
License Agreement Please read the following license agreen	nent carefully.		
END USER LIC	ENSE AGR	EEMENT	
IMPORTANT-READ CAREFULLY: T Gemplus software ("EULA") is a legal a the subsidiary or affiliate of Gemplus Ir version of the Software (as defined bel "You" are a person or legal entity wish governs your use of all of the Software "Software" means all computer software materials and any accompanying "onlin you hereunder. By downloading, insta	his End-User Li and binding agr nternational S.A ow) under this I ing to use the S e distributed or o re, associated m ne" or electronic ulling, copying, 1	icense Agreement eement between y . that distributed t EULA ("Gemplus") oftware. This EUI delivered hereunde edia, any printed printed provi breaking any seal of	for ou and his). .A er. ided to on, or
C I accept the terms in the license agreem	ient		
\odot I do not accept the terms in the license \circ	agreement		
InstallShield			
	< <u>B</u> ack	<u>N</u> ext >	Cancel



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

GemSafe Standard Edition Destination Folder Click Next to install to this fo	n 5.0 Administrator - InstallShield Wi Ider, or click Change to install to a differen	t folder.
: Install ComSafe St	andard Edition 5.0.0 dministrator to:	
C:\Program Files\G	Gemplus\GemSafe Libraries\	<u>C</u> hange
InstallShield		
a novana nova	< <u>B</u> ack <u>N</u> ext >	Cancel

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

🛃 GemSafe	Standard Edition 5.0 Administrator - InstallShield Wizard
Installing The prog	GemSafe Standard Edition 5.0 Administrator ram features you selected are being installed.
15	Please wait while the InstallShield Wizard installs GemSafe Standard Edition 5.0 Administrator. This may take several minutes.
	Status:
	Registering product
InstallShield -	
	< <u>B</u> ack <u>N</u> ext > Cancel



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

🙀 GemSafe Standard Edition 5.0 Administrator - InstallShield	Wizard 🔀
InstallShield Wizard Completion Standard Edition 5.0 Administrator. wizard.	eted sfully installed GemSafe Click Finish to exit the
< <u>B</u> ack <u>F</u> in	ish Cancel

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

j <mark>ह</mark> GemSa	fe Standard Edition S	i.0 Administrator Installer I 🗙
<u>.</u>	You must restart your changes made to Gem Administrator to take e No if you plan to resta	system for the configuration Safe Standard Edition 5.0 Iffect. Click Yes to restart now or t later.
	Yes	No

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

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

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

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



Installing Microsoft Certificate Services

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



4. Click Certificate Services, and then click Next.

indows Components Wizard	
Windows Components You can add or remove components of Windows.	R
To add or remove a component, click the checkbr part of the component will be installed. To see wh Details.	ж. A shaded box means that only at's included in a component, click
Components:	
🗹 📻 Accessories and Utilities	4.5 MB 🔺
Generation Server	24.6 MB
🔲 📴 Certificate Services	1.4 MB
🔲 🛄 E-mail Services	1.1 MB
Eax Services	22 N MR 🗾
Description: Installs a certification authority (CA) to public key security programs.) issue certificates for use with
Total disk space required: 3.6 MB	Details
Space available on disk: 69656.5 MB	
< <u>B</u> ack <u>N</u> ex	kt> Cancel Help
and the second se	



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

CA Type Select the type of CA y	vou want to set up.			Ē
Enterprise root CA				
C Enterprise subordin	ate CA			
C Stand-alone root C/	4			
C Stand-alone subord	linate CA			
The most trusted CA	in an enterprise. Shoi	uld be installed b	efore any other CA.	
☐ <u>U</u> se custom setting	s to generate the key	pair and CA ce	tificate	

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

Microsof	t Certificate Services 🛛 🔀
1	After installing Certificate Services, the machine name and domain membership may not be changed due to the binding of the machine name to CA information stored in the Active Directory. Changing the machine name or domain membership would invalidate the certificates issued from the CA. Please ensure the proper machine name and domain membership are configured before installing Certificate Services. Do you want to continue?
	<u>Y</u> es <u>N</u> o



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

dows Components Wizard		
CA Identifying Information Enter information to identify this CA.		Ē
Common name for this CA:		
] Distinguished name suffix:		
DC=DemoPC,DC=com		
I Preview of distinguished name:		
CN=,DC=DemoPC,DC=com		
Validity period: 5 Years	Expiration date: 11/30/2010 10:33 A	M
< Back	Next > Ca	ncel Help

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

<u>C</u> ertificate database:		
C:\WINDOWS\system32\CertL	og	Br <u>o</u> wse
Certificate <u>d</u> atabase log:		
C:\WINDOWS\system32\CertL	og	Bro <u>w</u> se
Shared folder:		
		Blowse
1		



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

Windows Com	ponents Wizard	×
Configurin Setup is	g Components s making the configuration changes you requested.	B
6	Please wait while Setup configures the components. This may take several minutes, depending on the components selected.	
Status:	Building file list	
-		
	< <u>Back</u> <u>N</u> ext> Cancel +	ielp

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

Microsoft	: Certificate Services	×
1	To complete the installation, Certificate Services must temporarily stop the want to stop the service now?	Internet Information Services. Do you



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**.

	is <u>window ri</u> eip				
Console Root\Certificate	Templates				
Console Root	Template Display N	ame 🛆	Minimum Supported CAs	Version 🔺	
E 🎻 Active Directory Users	Exchange User		Windows 2000	7.1	
🗄 🙀 Certificate Templates	IPSec		Windows 2000	8.1	
E 📴 Certification Authority	IPSec (Offline request)		Windows 2000	7.1	
			Windows Server 2003, En	105.0	
	RAS and IAS Server		Windows Server 2003, En	101.0	
	Root Certification Authority Router (Offline request) Smartcard Logon		Windows 2000	5.1	
			Windows 2000	4.1	
			Windows 2000	6.1	
	Smartcard User		Windows 2000	11.1	
	Subordinate 🤇	Dyplicate Template	Windows 2000	5.1	
	Trust List Sigr	All Tasks	Windows 2000	3.1	
	User -		Windows 2000	3.1	
	User Signatur	Properties	Windows 2000	4.1	
		Liele		•	

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

General Reque nplate display name: I SmartCard User imum Supported CAs: Wind er you apply changes to this t ne. nplate name: ISmartCardUser idity period:	ows Server ; ab, you can	2003, Ent	Subject terprise Edition r change the	Name on e template
nplate display name: I SmartCard User imum Supported CAs: Wind er you apply changes to this t ne. nplate name: ISmartCardUser idity period: 1 years	ows Server ; ab, you can	2003, Ent no longei	erprise Edition	on e template
i SmartCard User imum Supported CAs: Wind er you apply changes to this t ne. mplate name: ISmartCardUser idity period:	ows Server ; ab, you can	2003, Ent no longer	erprise Edition	on e template
imum Supported CAs: Wind er you apply changes to this t ne. nplate name: ISmartCardUser idity period:	ows Server ; ab, you can	2003, Ent no longer	erprise Edition	on e template
antum supported CAS. wind ne. nplate name: ISmartCardUser idity period:	ab, you can	no longer	r change the	e template
er you apply changes to this t ne. mplate name: ISmartCardUser idity period: 1 years v	ab, you can	no longei	r change the	e template
nplate name: ISmartCardUser idity period: 1 years 💌				
ISmartCardUser idity period: 1 years 💌				
idity period: 1 years 💌	5			
idity period: 1 years				
1 years		1		
1 years 💌	<u>H</u> enewa	i perioa:		
	6	weeks	_	
D. H.C. L. and C. alla in Andrea I				
Publish certificate in Active L	лгестогу			
Do not automatically reer Directory	nroll if a dupli	icate certi	ificate exists	in Active
Directory				
		Car	ocal l	Applu



5.	Click the	Req	uest	Hane	dling	tab.
----	-----------	-----	------	------	-------	------

Issuance Requ General	irements Superseded Templates Extensions Securil Bequest Handling Subject Name
General	Subject Name
<u>P</u> urpose:	Signature and encryption
	Archive subject's encryption private key
	Include symmetric algorithms allowed by the subject
	Delete revoked or expired certificates (do not archive)
Minimum keu s	izer 1024
Minimum Key a	126. 1024
All <u>o</u> w priva	te key to be exported
Do the followir associated wit	te key to be exported ig when the subject is enrolled and when the private key h this certificate is used: ect without requiring any user input
Allow privation Allow privation of the following associated with <u>Enroll subjections of Prompt the</u>	te key to be exported ig when the subject is enrolled and when the private key h this certificate is used: ect without requiring any user input user during enrollment
 Allow privation Do the following associated with Enroll subject Prompt the private key 	te key to be exported ig when the subject is enrolled and when the private key h this certificate is used: ect without requiring any user input user during enrollment gser during enrollment and require user input when the is used
 Allow privation Allow privation Enroll subjeries Prompt the private key To choose whe (CSPs) should 	te key to be exported ig when the subject is enrolled and when the private key in this certificate is used: ect without requiring any user input user during enrollment user during enrollment and require user input when the is used ich cryptographic service providers be used, click CSPs.

- 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.

Group or user names: G Administrator (Administrator@MVALTES Authenticated Users	T)	
Authenticated Users		
🗖 Domain Admins (MVALTEST\Domain A	(dmins)	
Enterprise Admins (MVALTEST\Enterprise	ise Admins)	
	61.0234765360 5 66	
	- A-11	I
	A <u>a</u> a	Hemove
Permissions for Authenticated Users	Allow	Deny
Full Control		
Read		
Write		
Write Enroll		
Write Enroll Autoenroll		

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.

🚡 Console1				
Eile Action View Fa	vorites <u>W</u> indow <u>H</u> elp			
⇔ → 1 🖬 🖻	😫 💷 🕨 🔳			
🚡 Console Root\Certif	ication Authority (Local)			
Console Root	Name	Description		
Active Directory L Active Directory L Certificate Temple Certification Auth ThinClentRoo ThinClentRoo Pending R Pending R Certificate	Isers ThinClientRootCA	Certification Authority		
	New Window from Here			
	Refresh			
Enable additional Certifi	Help	on Authority	li	

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

Name	Intended Purpose	
Authenticated Session	Client Authentication	
🙀 CA Exchange	Private Key Archival	3
🙀 CCI SmartCard User	Smart Card Logon, Client Authentication, Secure Email	
🙀 CCI Smartcard Logon	Smart Card Logon, Client Authentication	
CEP Encryption	Certificate Request Agent	
🙀 Code Signing	Code Signing	
🙀 Cross Certification Authority	<all></all>	
🙀 Enrollment Agent (Computer)	Certificate Request Agent	
🙀 Exchange Enrollment Agent (Offline request)	Certificate Request Agent	
🗱 Exchange Signature Only	Secure Email	_
Vol Evohange Liser	Secure Email	



Configuring Microsoft Certificate Authority to Issue Smart Card User Certificate

1. Click Start > Administrative Tools > Certification Authority.

📴 Certification Authority			
Eile Action View Help			
Certification Authority (Local)	Name	Description	
E DemoCA	DemoCA	Certification Authority	1

2. Expand the defined CA.

📴 Certification Authority			
Eile Action View Help			
Certification Authority (Local)	Name	Description	
E- E DemoCA Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates	DemoCA	Certification Authority	

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



Name	Intended Purpose	
Authenticated Session	Client Authentication	
🙀 CA Exchange	Private Key Archival	
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	
🙀 Exchange User	Secure Email	_
1PSec	IP securitu IKE intermediate	_

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

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

Microsoft Certificate Services - Microsoft Internet Explorer		2 ×
Ele Edit Vew Favorites Iools Help		
🕒 Back + 🕗 - 💌 😰 🐔 🔎 Search 🎲 Favorites 😻 Media 🕐 😥 + 🦕 🗔		
Agdress 👔 http://localhost/certsrv/	💌 🔁 Go	Links 30
		1
Microsoft Certificate Services DemoCA	н	ome
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 ve identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate y perform other security tasks.	rify your ou request	ι.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (or view the status of a pending request.	RL), or to	
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		
		-
		-
Done	Local intranet	_



6. Select advanced certificate request.

Microsoft Certificate Services - Microsoft Internet Explorer	
le Edit Vew Favorites Iools Help	
) Badi. + 🔘 - 💽 😰 🐔 🔎 Search 🎲 Favorites 🜒 Media 🔗 🍰 + 🦕 🗔 -	
járess 👜 http://localhost/certsrv/certrqus.asp	💌 🄁 Go 🛛 Links
Microsoft Certificate Services DemoCA	Home
Paquast a Cartificata	
request a Gerundate	
Select the certificate type:	
User Certificate	
Or submit as advanced contificate request	
ur, suomit an <u>auvanceu certificate request</u> .	
r, submit an advanced certificate request.	

7. Select Create and submit request to this CA.





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

Microsoft Certific	ate Services - Microsoft Internet Expl	orer and a second s	
Ele Edit View F	Fgvorites Iools Help		27
🔾 Back 🔹 🔿 🗉 💽	👔 🐔 🔎 Search 🎲 Favorites 🐧	🖥 Meda 😧 🍙 - 🐛 🗔	
Address 💽 http://loc	calhost/certsrv/certrgma.asp		💌 🛃 Go Links 🕈
Microsoft Certific	ate Services DemoCA		Home
Advanced Ce	rtificate Request		
Certificate Temp	alate:		
	Enrolment Arent	r	
	Administrator	7	
Key Options:	Basic EFS		
	EFS Recovery Agent	ting key set	
CSP:	Smartcard Logon	pvider v1.0 •	
Key Heare	Smartcard User		
Key Usage.	User Subordinate Certification Authority		
Key Size:	Web Server	12 1024 2048 4095 8192 16284)	
	Automatic key container name	C User specified key container name	
	Mark keys as exportable		
	Export keys to file		
	Enable strong private key protect	on	
	Store certificate in the local comp	uter certificate store	
	Stores the certificate in the local	computer store	
	instead of in the user's certificate install the mot CA's certificate	e store. Does not /ou must be an	
	administrator to generate or use	a key in the local	
	machine store.		
Additional Optio	ns:		
Request Format:	CMC CPKCS10		
Hash Algorithm:	SHA-1 💌		
	Only used to sign request.		
	Save request to a file		
a .			Local intranet

- 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**.

Microsoft Certificate Services - Microsoft Internet Diplorer	
Ele Edit View Favorites Iools Help	2
😮 Back + 🕥 - 📧 😰 🐔 🔎 Search 🌸 Favorites 💐 Media 🕐 🍰 + 😓 🗔	
Address 😸 http://localhost/certsrv/certrgma.asp	💌 🔁 Go 🛛 Links 🏻
	-
Microsoft Certificate Services DemoCA	Home
Advanced Certificate Request	
And the set the data	
Certificate Template:	
Enrollment Agent	
Key Ontione:	
Consta new law ant	
CSD: Microsoft Enhanced Countegraphic Develops of Dire	
Key Ileaner @ Simplus	
May Come 1004 Mill: 384 commentary for some find and states	
Key Size: 1024 Mac16304 (common wy size: 512 (size shee sheet)	
Automatic key container name C 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 install the root GA's certificate. You must be an administrator to generate or use a key in the local machine store.	
Additional Options:	
Request Format: @ CMC O PKCS10	
Hash Algorithm: SHA-1 Only used to sign request.	
□ Save request to a file	
2	
	Local intranet

- 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.

Microsoft Certificate Services - Microsoft Internet Explorer	X
Ele Edit View Favorites Iools Help	27
🔾 Back + 🔘 - 💽 😰 🐔 🔎 Search 🤹 Favorites 🔮 Media 🔗 🍰 🍃 🗔	
Address 👩 http://localhost/certsrv/certfrish.asp	💌 🄁 Go 🛛 Links 🏁
Microsoft Certificate Services DemoCA	Home
Certificate Issued	
The certificate you requested was issued to you.	
Install this certificate	



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



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

Microsoft Certificate Services - Microsoft Internet Explorer	
Ele Edit View Favorites Iooks Help	27
🔾 Back + 🔿 - 💽 😰 🏠 🔎 Search 🎲 Favorites 👋 Media 🔗 🍰 🖓 🗔	
Agdress 👩 http://localhost/certsrv/certmpn.asp	💌 🔁 Go 🛛 Links 🏁
Microsoft Certificate Services DemoCA	Home
Certificate Installed	
Your new certificate has been successfully installed.	



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.

Lee See See Partices Loss See Search Parontes Proventes Proventes Proventes Proventes Proventes Proventes Proventes	💌 🋃 🐼	Links
Stat. • O • • 2 • Starch • Pavones • Meda • O • • C Lat deres • http://localhost/certsrv/certsces.asp Microsoft Certificate Services Smart Card Certificate Enrollment Station Enrollment Options:	💌 🋃 😡	Links
Microsoft Certificate Services Smart Card Certificate Enrollment Station Enrollment Options:	Ho	me
Microsoft Certificate Services Smart Card Certificate Enrollment Station Enrollment Options:	Ho	me
Smart Card Certificate Enrollment Station		
Enrollment Options:		
Enrollment Options:		_
Certificate Template: Smartcard User 💌		
Certification Authority: Smartcard Logon		
Cryptographic Service Provider: Gemplus GemSAFE Card CSP		
Administrator Select Certificate		
Jser To Enroll:		_
(No user selected) Select User		
itatus:		_



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

Back + · · · ·	succes Toos Geb		
Address (a) here the at	A Canch Cancher of Marks 21		
the second se	A	- 63 co Lois *	
Microsoft Centre of	ta Sericore trificate Enrollment Station	Ustur	
Enrollment Option			
Cert Cert Si	Ricate Template Smartcard User Smartcard User Cryptographic Smartcard Logen Cryptographic Gemplus GemSAFE Card CSP Administrator Administrator Pulministrator		
User to Enree:	Ptiruter selected) Select User		
Status:	elect User		? ×
Please selec	Select this object type:		
-	User	Object Type	s
	From this location:		
	Entire Directory	Locations.	
	Enter the object name to select (examples):		
		Check Nam	es
a	Advanced	1 Canad	- 1

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

Microsoft Smart Card Enrollment Station - Microsoft Internet Explorer		
Ele Edit Yew Favorites Iools Help		
3 Badi + 🔿 - 💽 👔 🐔 🔎 Search 🎲 Favorites 🔮 Media 🔗 🎰 🍃 🕞		
Address 🛃 http://localhost/certsrv/certsces.asp		💌 🛃 Go 🛛 Links 👌
Microsoft Certificate Services		Home
Smart Card Certificate Enrollment Station		
Enrollment Options:		
Certificate Template: Smartcard User		
Certification Authority: DemoCA -		
Cryptographic Gemplus GemSAFE Card CSP		
Administrator Signing Certificate:	Select Certificate	
User To Enroll:		
SCUser1@DemoPC.com	Select User	
Status:		
Please incert the user's smart card into a reader and then proce 'Enrol!		
Please insertine user's smart card into a reader and then press chron.		
		Enroll



Testing the Smart Card

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



2. Select Certificates.

InSale			GEMPLI
A second second	Certificates		1
Card Contents		PIN Code	: Lige
Certificates		- 🔯 Texas Instruments SmatCastSkt 0	
and Properties			
	2		
ed Administration		Firmideau Eme	Security and
ware Administration		interior interior	Heater 25
Diagnostic/Help			



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

Toolbox		B GEMI-L
Card Contents	Certificates	
2		PIN Code: Lagout
Cettilicates		E 🍋 Texas Instruments SmatCardSlot 0
50		SC Test 1's ID BSA Public Key 1024 bits
Card Properties		S RSA Private Key 1024 bits
	STAN AT	
	CARL 9 2011	
Card Administration	19/1 B 8/1	Shink details. Entries Set us detailst
oftware Administration	X 2.70 7.8	Import. Exase All Register All
Discussion & Late		

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

	Diagnostic Tool		-
Card Contents Card Administration Software Administration Diagnostic/Help Diagnostic Tool	18:	#<	
	Pasameter	Value	



5. Select the Smartcard and readers diagnose button.

10010-0H	Diagnostic Tool		
Card Contents Card Administration Software Administration Diagnostic/Help	⊞ 💋 System into ⊞ 📁 GemSafe Librarie	E	
Diagnostic Tool	Paismeter	Value	
	- -		

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

Gemplus SmartDiag v2.1	×
Ŕ	Welcome to Gemplus SmartDiag v2.1.
	This program verifies that smart card readers and the cards they contain are available to other programs.
	If the diagnostic utility identifies a problem, it reports the most likely cause and gives the necessary information to correct the situation.
	Click Start to begin the diagnostic.
8	<u>Start</u> Cancel



You should receive the following PASSED response.

😪 Gemplus SmartDiag v2.0	X
	PASSED
	The reader and the card it contains are OK.
	Click Class to finish the disgnestic session
	Cilck Close to finish the diagnostic session.
<u>A</u> dvanced View	<u>N</u> ext>

Creating Customized User Install Packages for Clients PCs (Optional)

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

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

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

To change RAMDisk siz	e, click Start >	Control Panel >	HP RAMDisk Manager.
-----------------------	-------------------------	-----------------	---------------------

🛙 HP RAMDisk Manager 🛛 🛛 🔀
🕪 RAMDisk (Z:)
HP RAMDisk Manager
2 MB 64 MB
64 MB
OK Cancel Apply



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

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

s	ystem Properties Environment Variables ?	×
	General Computer Name Hardware Advanced Rer You must be logged on as an Administrator to make mos Variable Value Performance Visual effects, processor scheduling, memory usage, a TEMP C:\Windows\Temp	
Control Panel File Edit View Pavor	User Profiles Desktop settings related to your logon System variables Variable Value)
Address Control Panel	Startup and Recovery CommonProgra C:\Program Files\Common Files System startup, system failure, and debugging informat ComSpec C:\WINDOWS\system32\cmd.exe DEVICEMODEL {0000000-0000-0000-0000-0000-0000-0000)
Help and Support	OK Cancel Apply Image: Concel Image: Conc	
	USB Storage Security	

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



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

Gem Safe	
Card Contents	
Certificates	
80	
Card Properties	
Card Administration	
Software Administration	
Diagnostic/Help	

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

Gem Safe	DIN Doligy	
Card Contents Card Administration Software Administration	File selection	Browse
GemSafe Configuration PIN Policy GemSafe User Setup	PIN Policy Rules PIN: User Image: PIN Policy Image: PIN Policy PIN minimum length: Image: PIN maximum length: PIN maximum length: PIN maximum length: PIN maximum length: Image: PIN maximum length: PIN m	Add
Diagnostic/Help	Save as	Save



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

Save As				1	?	×
Save jn:	📋 My Documen	ts	•	0 🖸 🛤	 •	
My Recent Documents Desktop My Documents My Computer	TCUser1.ppc					
My Network Places	File <u>n</u> ame: Save as <u>typ</u> e:	Pin Policy Config	uration (*.ppc)	• •	<u>S</u> ave Cancel	

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

GemSafe		🖉 GEMPLUS' 👔
100100x	GemSafe Configuration	a
Card Contents		
Card Administration	File Selection	
Software Administration		Browse
FIN Policy	User Features Selection Certificate Feature User can erase objects on the card Import / export certificates allowed	Certificate Registration Tool Feature Certificate registration allowed Change PIN popup allowed
2	PIN Management Feature	GemSafe ToolBox Feature
GemSafe User Setup	 User can unblock smart card User can remotely unblock connected smart card ✓ Change User PIN(s) allowed Change Admin PIN allowed 	3000 Display timeout (ms) Save as Save
Diagnostic/Help	[



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

Save As						<u>?</u> ×
Save jn:	📋 My Documer	ts	•	6 🕫	产 🖽 •	
My Recent Documents Desktop	國 hp.gsl 國 TCUser1.gsl					
My Documents My Computer My Network Places	File <u>n</u> ame: Save as <u>t</u> ype:	hp hp.gsl			•	<u>S</u> ave Cancel

Select Libraries User Setup in the left frame, and then define Libraries User Setup.
 NOTE: You must select CSP if you are operating in a Microsoft environment.

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

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

	GemSate User Se	stup				2
Card Contents						
Card Administration	File Selection					
Software Administration					1	vowse
GenBale Configuration	Oypto Modules El RicSett El CSP	Tokens	V1 Applet V2 Applet	Gend IN IN IN IN IN IN IN IN IN IN IN IN IN	isfe Tooblox entificate Tool and Properties Too IN Management To ocumentation Too agnostic Tool	al aol I
GentSafe User Setup	Registration Tool	Real P (P s	ders Vrivers imartDiag		Languages English	×
	3	22		0		Next >>



iemSate		GEMPLUS
TODIOGR	GemSafe User Setup	De .
Card Contents	- Castlein Teather Contacteding	
Card Administration	C Salada anaza	1 marsha
Software Administration	I_ spear screen	100000
28	Background	D'ancei
GeniSale Configuration	Small background	trowse
	T Tibe	Innou.
PIN Policy	File Selection Select a conferention file to include in the seture	
-	CODocuments and Settings/Administrator/Wy Documents/Pp	.osl Browse
GentSale User Setup	Select a DN roles file to include in the return	and the second second
	Colour and Setting Advantage (A)	Therefore Comment
	C (Locuments and Settings (Administratory my Documental in	Erowse
Discourse Alaba		<< Previous Next >>

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

	GemSafe User Setup	2
Card Contents		-
Card Administration	-Setup Location	
Software Administration	Sebup Name:	
38	Pputer	
Carallina Caralina antina	Setup Path	
sensare comparation	COProgram Plant Converting Converting Converting Converting	_
	and the set of the set	
PIN Police	Change path	line
-	- Takes Couldre -	
-	Setup Creature	
Gem5ale User Setup	Create Setup	

10. Select $\ensuremath{\text{OK}}$. The new setup has been created.

Libraries	User Setup	×
į	New setup cre	ated
	OK	



The user package has been successfully created.

You can:

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

Additional Information

Using a Smart Card For Windows Network Login

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

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

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

Administration of the GemSafe Smart Card

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

Working with GemSafe Libraries

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

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



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

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

Usage cases

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

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

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

Advanced General	Automatic Updates H	Remote lardware
Windows use on the netwo Computer <u>d</u> escription:	es the following information to identify your rk.	computer
Full computer name:	For example: "IIS Production Server" of "Accounting Server". mval.MVALTEST	T
Domain:	MVALTEST	
To rename this comput Note: The identification • The Certification Auth	er or join a domain, click Change.	hange
To rename this comput Note: The identification • The Certification Auth	er or join a domain, click Change.	hange
To rename this comput Note: The identification • The Certification Auth	er or join a domain, click Change.	hange
To rename this comput Note: The identification • The Certification Auth	er or join a domain, click Change.	hange

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



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

ug on i	
Copyright Co Haussial Co	ives-2001 Iversitian Microsoft
PIN:	[<u> </u>
	OK Carcel Stut Dawn Dotions <<

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

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

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

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

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

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

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

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

1. Log out of the RDP session.



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

(p)	PC Session Allocation © 2006 Hewlett-Packard Development (n Clier
		v1
5AM 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 t	to Windows	-
Copyright © Microsoft Co	1985-2001 rporation	Microsoft
PIN:	OK Cancel Shut Down Or	otions <<

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

Usage case 4: Accessing secure Web site

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

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





- 4. In Internet Explorer, type the address of a secure Web site.
- 5. If the system displays security alert messages, click OK.

The LED on the card reader indicates when the Web site is accessing the smart card to verify whether the certificate is approved for the site.

6. After the secure Web site displays, a lock icon in the lower right corner of Internet Explorer confirms that you are connected to a secure Web site.



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

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

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



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



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

📴 New Connection Wizard	ı 🔀
	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.

Work	Propert	ies			2
eneral	Options	Security	Networking	Advanced	
lost na 57.54.	nme or IP a 0.1):	iddress of	destination (su	ich as microsoft.	com or
/pn.wo	ork.net				
First c	onnect -				
Win Inter	dows can net, befor	first conne e trying to	ect the public r establish this v	ietwork, such as rirtual connectior	the 1.
)ial anothe	r connect	ion first:		
					Y
Sho	w icon in r	notification	area when co	nnected	
					Cano
			L		Caric

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:		
l.		
	ОК	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.



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

1. Click the Citrix Program Neighborhood desktop shortcut.



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





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

ICA Smart Card C	onnection Pro	perties	?×
Connection Options	Logon Information	Application	
 Local user Pass-through 	authentication		
C Smart card	authentication		
C User-specified cre	edentials		
User name:			
Password:			
Domain:			
🗖 Save passwo	rd		
	OK Car	ncel	Help

- 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.

Log On to Windows			
	/indows Serv	/er 2003	
Copyright © 1985-2003 Microsoft Co	ingen her		Recession 1
User name:		_	
Password:	Terrori 1 the		



Service and Support

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

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

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

Phone: (888)-343-5773.

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



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