Version 7.0 09/11



Xerox[®] Smart Card Installation Guide

Xerox® WorkCentre 5632/5638/5645/5655/5665/5675/5687 Xerox® WorkCentre 5735/5740/5745/5755/5765/5775/5790 Xerox® WorkCentre 5135/5150 Xerox® WorkCentre 5030/5050 (software version 05.004.xx.xxx)



© 2011 Xerox Corporation. All Rights Reserved. Unpublished rights reserved under the copyright laws of the United States. Contents of this publication may not be reproduced in any form without permission of Xerox Corporation.

XEROX® and XEROX and Design® are trademarks of Xerox Corporation in the United States and/or other countries.

Changes are periodically made to this document. Changes, technical inaccuracies, and typographic errors will be corrected in subsequent editions.

Document version 7.0: September 2011

Table of Contents

1 Introduction

| | Compatibility |
|---|--|
| 2 | Preparation |
| | Server Specifications10Electrical Requirements10 |
| 3 | Installation |
| | Software Enablement12Configuring the Smart Card13Hardware Installation26Using the Smart Card34 |
| 4 | Troubleshooting |
| | Fault Clearance36Locating the Serial Number36Troubleshooting Tips37During Installation:37After Installation:38 |
| А | Retrieving the Certificate from a Domain Controller or OCSP Server |

B Determining the Domain in which your Card is Registered

4 Xerox® Smart Card Installation Guide

Introduction

The Xerox *Smart Card* solution brings an advanced level of security to sensitive information. Organizations can restrict access to the walk-up features of a Xerox device. This ensures only authorized users are able to copy, scan, e-mail and fax information.

The key benefit of this solution is its two-factor identification requirement. Users must insert their access card and enter a unique Personal Identification Number (PIN) at the device. This provides added security in the event that a card is lost or stolen.

Once validated, a user is logged into the Xerox device for all walk-up features. The system allows for functions to be tracked for an added layer of security.

The Xerox *Smart Card* enablement kit integrates with Xerox multifunction printers and existing smart and personal identity verification cards and readers.

This guide explains how to install and configure the *Smart Card* solution. It identifies the resources and equipment required to complete a successful installation.

Should you require any further information, please contact your Local Xerox Representative.

Compatibility

This solution is compatible with the following product and configurations:

| Configuration | Software Level |
|---|--|
| Xerox WorkCentre 5030/5050 Multifunction ^a | 05.004.xx.xxx |
| Xerox WorkCentre 5632/5638/5655/5665/5675/5687 Multifunction | 21.113.xx.xxx ^b 21.120.xx.xxx 25.054.xx.xxx |
| Xerox WorkCentre 5135/5050 Multifunction | 21.120.xx.xxx |
| Xerox WorkCentre 5735/5740/5755/5765/5775/5790 Multifunction | 06x.130.xxx.xxxxx 06x.131.xxx.xxxxx |

a. If your machine has software level 05.003.xx.xxx, the *Smart Card* software can not be installed without first upgrading the machine software. Please contact your Xerox Representative for details.

b. If your machine has software level 21.113.02.070 or lower, the *Smart Card* software can not be installed without first upgrading the machine software. Please contact your Xerox Representative for details.

To identify the software level on your machine, perform the following steps:

- 1. Press the Machine Status 🔀 button on the control panel.
- 2. Information about the machine is displayed. If necessary, select **Machine Details** to display the *System Software Version* number.

Card Readers and Card Types

Supported Card Types

The customer is responsible for purchasing and configuring the access cards. The following card types are recommended:

- Gemalto TOP DL GX4 144K V2.6.2b Applets
- Oberthur ID-One Cosmo v5.2 128K V2.6.2 Applets
- Oberthur ID-One Cosmo v5.2 72K V2.6.1 Applets
- Oberthur ID-One Cosmo v5.2D 72K V2.6.1 Applets
- Oberthur ID-One Cosmo v5.2 72K V2.6.2 Applets
- Gemalto GemCombiXpresso R4 dual interface 72K V2.6.2 Applets
- Axalto Access 64KV1
- Axalto Access 64KV1
- Gemplus GXP3 64V2N V2.6.1 Applets
- Gemalto Cyberflex Access V2C 64K V2.6.1 Applets
- Oberthur ID-One Cosmo V5.2D 64K
- Oberthur OCS Galactic V1 32K V1 Applets
- Oberthur Cosmo V4 32K V1 Applets
- Schlumberger / Axalto Cyberflex V2 32K V1 Applets

Other card types may function with the solution, but have not been validated. Supported Card Types

Supported Card Readers

The customer is responsible for providing a card reader for each Xerox device. The following card readers are compatible with the solution:

- Gemplus GemPC USB SL
- Gemplus GEMPC Twin
- SCM Micro SCR3310
- SCM Micro SCR3311
- OmniKey Cardman 3021 USB
- OmniKey Cardman 3121 USB
- ActivCard USB Reader V2 with SCR-331 firmware

Other CCID compliant readers may function with the solution, but have not been validated.

Note: Information about CCID compliant card readers can be obtained from various websites, for example www.pcsclite.alioth.debian.org/ccid.This site is not a Xerox website and is not endorsed by Xerox.

Documentation and Support

For information specifically about your Xerox product, the following resources are available:

- **System Administrator Guide** provides detailed instructions and information about connecting your device to the network and installing optional features. This guide is intended for System/Machine Administrators.
- User Guide provides detailed information about all the features and functions on the device. This guide is intended for general users.

Most answers to your questions will be provided by the support documentation supplied on disc with your product. Alternatively you can contact the Xerox Support Center or access the Xerox website at www.xerox.com.

Preparation

This section explains the preparation and resources required to install the Smart Card.

The installation will take approximately one hour for each device. The following items are required in order to complete the installation:

| Item | Supplier |
|--|----------|
| Compatible Card Reader (refer to Supported Card Types on page 7) | Customer |
| Compatible Access Card (refer to Supported Card Types on page 7) | Customer |
| Smart Card enablement kit 498K17544 (one for each Xerox device) | Xerox |
| Feature Enable Key | Xerox |
| TCP/IP enabled on the device | Customer |
| DNS Host name or static IP address assigned | Customer |
| Network Settings to be checked to ensure network is fully functional | Customer |
| Domain Controller (DC) information: Domain Controller authentication environment IP address or Host Name Domain information Domain Controller Root and Intermediate certificates Check that all certificates are in 64 bit X.509 format Determine if the DC is registered with the OCSP at this site | Customer |
| Online Certificate Status Protocol (OCSP) Server Information: OCSP Server URL OCSP - Root and Intermediate Certificates Check that all certificates are in 64 bit X.509 format | Customer |
| Proxy Server configuration details | Customer |

To set up the Domain Controller (DC) validation, you will need to determine if your site validates the DC against the Online Certificate Status Protocol (OCSP) server. Many sites use OCSP to validate individuals, but do not register the DC with it. If you set up the Xerox device to validate the DC and it isn't registered, the procedure will fail.

If your site does register the DC with OCSP, you will need to decide whether:

- to validate the DC against OCSP before validation of the user, or
- to validate the DC after validation of the user

The first method requires installation of the DC certificate as part of this procedure and is the more accepted method for validation. The second method retrieves the DC certificate automatically for each authentication and doesn't require installation of the DC certificate onto the Xerox device.

An additional option is to combine the first and second options and compare the retrieved DC certificate to the one stored at installation. This provides the most security as it prevents rogue DCs masquerading as the real DC.

Note: Certificates are often obtained from the Information Technology professionals that support your organization. If you are unable to obtain the required certificates, refer to the process outlined in Appendix A. You can determine the domain that you are registered in using the process outlined in Appendix B.

Server Specifications

Prior to installation, ensure your network infrastructure supports *Smart Card* or *Personal Identification Verification (PIV)*.

Names or IP addresses of all servers and domains are required during setup.

Electrical Requirements

The USB port on the back of the Xerox device network controller provides the power required for any of the supported card readers.

Installation

This section provides instructions for installing and configuring the *Smart Card* solution.

There are 4 main installation procedures to follow in sequence.

- Software Enablement Use the Feature Enable Key to enable the *Smart Card* to be configured.
- **Configuring Smart Card** Enabling the *Smart Card* function and customizing the settings.
- Hardware Installation Unpacking the *Smart Card* Enablement kit and installing the card reader device.
- Using Smart Card Instructions on how to use the card reader device to access the device functions.

Software Enablement

Prior to installing the *Xerox Smart Card* solution, the software requires enabling on your Xerox device using Internet Services. The Feature Enable Key is printed on the inside cover of the Enablement guide provided within the *Xerox Smart Card* kit.

Follow the instructions below to enable the device software:

Xerox WorkCentre 5632/5638/5655/5665/5675/5687, Xerox WorkCentre 5135/5150 and Xerox WorkCentre 5030/5050:

- 1. Access **Tools** at the device
 - a. At the Xerox WorkCentre, press the **Access** button on the control panel.
 - b. Enter the appropriate User ID and Password to access **Tools**.

Note: The default user name and password are: admin and 1111.

- c. Select Go to Tools.
- 2. Enable the Smart Card Software
 - a. Select More to access additional Tools options.
 - b. Select **Optional Services**. If necessary, use **More** to navigate to the option.
 - c. Select Smart Card. If necessary, use More to navigate to the option.
 - d. When prompted, select the **Option Kit Number** entry box and enter the unique *Feature Enable Key* provided on the inside cover of the *Smart Card Enablement Guide*.
 - e. Select **Exit Tools**.

Xerox WorkCentre 5735/5740/5755/5765/5775/5790:

- 1. Access **Tools** at the device
 - a. At the WorkCentre, press the Machine Status button on the control panel.
 - b. Select the **Tools** tab.
 - c. Enter the appropriate User ID and Password to access **Tools**.

Note: The default user name and password are: **admin** and **1111**.

- 2. Enable the *Smart Card* Software
 - a. Select Service Settings.
 - b. Select Optional Services.
 - c. Select Smart Card.
 - d. When prompted, select the entry box and enter the unique *Feature Enable Key* provided on the inside cover of the *Smart Card Enablement Guide*.
 - e. Select Enter.
 - f. Reboot the device (the device may automatically reboot).

Once the reboot is complete, the *Smart Card* function is ready to be configured using the *Internet Services* interface.

Note: No services will be restricted until Smart Card has been configured using Internet Services.

Configuring the Smart Card

Once the *Xerox Smart Card* feature has been enabled on the device it can be configured using Internet Services.

Follow the instructions below to enable and configure the Smart Card:

1. Access Internet Services

- a. Open the web browser from your Workstation.
- In the URL field, enter http:// followed by the IP Address of the device. For example: If the IP Address is 192.168.100.100, enter the following into the URL field: http://192.168.100.100.

| Status Jobs Print Scan | Properties Support |
|--|--|
| Status Welcome | Welcome! |
| Description & Alerts Billing Information Usage Counters Configuration Consumables Trays | Welcome to your new Werk/Center, You will have reserved several packages of documentation materials, which are design before proceeding with the device installation. For additional information, documentation, the latest print drivers and much more visit: <u>http://www.warsw.com</u> |
| | Don't Show Welcome Page Again |

c. Press Enter to view the Home page.

2. Access Properties

- a. Select the **Properties** tab.
- b. If prompted, enter the Administrator User ID and Password. The default is **admin** and **1111**.
- c. Select the **Login** button.
- 3. Configure the date and time to update automatically
 - a. Select Connectivity.
 - b. Select **Protocols** and then **NTP**.

Note: A pop-up window may appear requiring you to login.

c. Ensure the **NTP Enabled box** is checked for the *Network Time Protocol* option, then enter the *IP Address* or the *NTP Host Server Name*.

In most cases this will be your DHCP server, and it will provide the time in Greenwich which must be corrected for your time zone by the GMT offset.

| Internet Services | | | | | XEROX WorkCentre 5030 | | | | Eð sam | nin - togour (Ho | | |
|---|----------------------------------|-------------------|------|---|-----------------------|-------------|-----------|--|---------|-------------------|----------|-----|
| Status | Jobs | Print | Scan | 1 | Properties | Support | | | | | | |
| Propertie | 15 | | | ^ | NTP | | | | | | | |
| Configura | ation Ove | rview | | | Offect of | Local Time | 2000 | | | | | |
| •General | Setup | | | | onseco | Local Thile | zone | | | | | |
| Connect Physics Protocs Apple1 | ivity al Conne ols Talk | ections | | | Offset of -4.0 ¥ | Greenwich | Mean Time | | | | | |
| NetWa | re | | | | Network | Time Proto | ol | | | | | |
| IP (Int SLP SNMP SSDP Micros | oft Netwo | otocol) orking | | | NTP Enab | bled | .01 | | | | | |
| Raw T | CP/IP Pri | inting | | | 10 10 v4 | addraee | | | IP Addr | ess: Port | | |
| LDAP | server | | | | O Host | Name | | | 111 | . 222 | . 33 | . 3 |
| HTTP | setup | | | | | | | | Barkun | ID Addres | s · Port | |
| Proxy | Server | | | | | | | | - Chup | 1. | | |
| NTP | | | | | | | | | 0 | . 0 | . 0 | . 0 |
| + Services | F | | | | | | | | | | | |
| F-mail | 9 | | | | | | | | | | | |
| +Interne | et Fax | | | | | | | | | | | |
| Networ | k Scann | ning | | | | | | | | | | |
| • Scan to | Home | a | | | | | | | | | | |
| * Reprint | Servic | JODS | | | Note | | | | | | | |
| Le us | - servic | | | ۷ | | | | | | | | |
| | | | | | 1 | | | | | | | |

- d. At the Offset of Local Time Zone option select the GMT offset that is correct for your region.
- e. Select **Apply**. The device may reboot.

Note: The sign in front of the number is important. Most of Europe is plus of Greenwich Mean Time, while North America is minus. Please consider the implications of Daylight Savings Time when selecting the Offset of Local Time Zone option.

Note: If Network Time Protocol is not available, check that the time set on the device matches the network time on the Domain Controller Authentication Server.

To determine the network time, view the time as displayed on your computer. To observe or set the time on the machine use the following instructions:

Note: If using Network Time Protocol (NTP) do not change the time on the device. The device will obtain the time from the NTP server.

WorkCentre 5632/5638/5655/5665/5675/5687, Xerox WorkCentre 5135/5150 and Xerox WorkCentre 5030/5050:

- a. At the Xerox WorkCentre, press the Access button on the control panel.
- b. Input your User Name and/or Password.
- c. Select Go to Tools.
- d. Select System Settings.
- e. Select Time and Date.
- f. Select Set Date and Time.
- g. Select Set Time.
- h. Observe the time and if it is not correct, validate that the GMT offset is correct for your region.

Note: If any changes are made, the device will automatically reboot.

WorkCentre 5735/5740/5755/5765/5775/5790:

- a. At the WorkCentre, press the Machine Status button on the control panel.
- b. Select the **Tools** tab.
- c. Enter the appropriate User ID and Password to access **Tools**.

Note: The default user name and password are: admin and 1111.

- d. Select Device Settings.
- e. Select General.
- f. Select Date & Time.
 - Date: Select the Format required and enter the Month, Day and Year.
 - **Time**: Enter the correct Hour and Minutes and select PM or AM. If a 24 hour clock is required, select the 24 hour clock option and enter the Hour and Minutes using the 24 hour clock format.
 - **GMT Offset (Time Zone) (System Software 06x.130.xxx.xxxx)**: Use this option to set the difference between your local time and Greenwich Mean Time. Enter the GMT Offset time between -12.0 and 14.0 hours using the arrow buttons.
 - **Time Zone (System Software 06x.131.xxx.xxxx):** Touch the **Time Zone** drop down menu and select the correct time zone for your device's locale. The machine time is automatically adjusted if daylight savings is in effect in your time zone.
- g. Select **Reboot** to save and reboot the device.

4. Access CAC configuration settings

The next steps vary depending on which Xerox WorkCentre model you have.

- For Xerox WorkCentre 5030/5050 refer to page 15.
- For Xerox WorkCentre 5632/5638/5655/5665/5675/5687, Xerox WorkCentre 5135/5150 and Xerox WorkCentre 5735/5740/5755/5765/5775/5790 refer to page 16.

Xerox WorkCentre 5030/5050:

a. Select Security and select Authentication Configuration.

Note: If this is the first time you are entering the authentication wizard, you may be prompted to enter a password.

b. Enter the password and select **Next**.

| Internet Sei | vices | | XEROX Wo | orkCentre 5030 |
|--|---|------------|---------------------------------|---|
| Status Jobs | Print | Scan | Properties | Support |
| Properties Configuration O Description P General Setup P Connectivity P Services *Security | verview | | Authenticatio | n Configuration ice: System Administrator Password ad Carefully For security reasons, you must change the current system administrator's password from the factory default For security reasons, you must change the current system administrator's password from the factory default |
| User Data Enc Autherbashan IP Filtering Audit Log Machine Digita Management Trusted Certifi • On Demand I | onfigurati Configurati Certificate ate Authori Verwrite | on ties | User Name User Name admin | setting. INPORTANT Do not forget this password, or you could be completely locked out of the system, requiring a service call. e & Password e: (Not editable) |
| | | | Retype Ne | w Password |

c. Select Next.



d. Select CAC/PIV and select Next.



e. Select **Configure**.

The Authentication Configuration screen is displayed.



f. Enter the **Smart Card Timeout** required between 1 and 120 minutes.

The default setting is 5 minutes.

g. If the machine is inactive for the period of time specified, it will end the session automatically.

| nternet Services | XEROX WorkCentre 5050 | 👍 edmin - Legeut Home Index | Site Hap Help |
|--|---------------------------------------|--|-----------------|
| Status Jobs Print Scan | Properties Support | | |
| Properties Configuration Overview Description | Authentication Configuration | | |
| -General Setup Configuration Cloning Image Settings Internationalization Alert Notification | Current Configuration | Device User Interface Authentication CAC/PTV | dit Methods |
| Hactine Software *Connectivity Physical Connections *Protocols | Provice System Administrator Password | | Modity_ |
| AppleTalk NetWare 1P (Internet Protocol) SLP SNMP | CAC/PTV | P Configured | Edit |

Note: When the Smart Card is removed, the user session will timeout.

Xerox WorkCentre 5632/5638/5655/5665/5675/5687, Xerox WorkCentre 5135/5150 and Xerox WorkCentre 5735/5740/5755/5765/5775/5790 (System Software 06x.130.xxx.xxxx):

a. Select Security and select Authentication Configuration.

Note: If this is the first time you are entering the authentication wizard, you may be prompted to enter a new password that is different from the default password.

b. Enter new password and select **Next**.

| Internet Services | XEROX WorkCentre 5675 |
|---|--|
| Status Joks Print Scan | Properties Support |
| Properties Configuration Overvies Description *General Setap | Authentication Configuration Device System Administrator Password |
| Connectivity Services | Please Read Carefully |
| *Accounting *Security User Deta Encryption Addresitation Configuration *User Enformation Database | Par administre senses, you must change the current system administrative gassword from the factory default setting. The administrative control of the current system administrative gassword from the factory default setting. The red forget this password, or you could be completely located and of the system, sequence a set. |
| DP filtering Audit Log | User Name & Password |
| Hachine Digital Certificate Management Disec | User Name (Not editable) admin |
| 802-1X *On Demand Overwrite | New Paymond |
| | |
| | Best |

c. Select Next.



d. Select the *Device User Interface Authentication* option **CAC/PIV** and select **Next**.

Note: This screen is dependent on the selection made on the previous screen.



e. Select the *Device User Interface Authentication* option **Configure**.

The *Authentication Configuration* screen is displayed.

f. Enter the **Smart Card Timeout** required between 1 and 120 minutes. The default setting is 5 minutes.

If the machine is inactive for the period of time specified, it will end the session automatically.

| Internet Services | XEROX WorkCentre 5675 | 1 ann - | Logout Horne Soder Site Hop Holp |
|---|--|------------------|--|
| Status Jaks Print Scan | Properties Support | | |
| Properties Canfouration Overview Description • General Satup | Anthentication Lonfiguration | | |
| *Services | Authentication - (Required) | | |
| *Accounting | Concepta Dear Interface Authentication | 1 tot Configured | Configura_ |
| User Data Encruption Authentication Configuration | Web Over Interface Authentication Locally on the Device (Internal Database) | and the second | Yere- |
| 17 Filtering | Authorization Configuration | | |
| Audit Log Machine Digital Certificate | Local User Information Database | | View- |
| IFtet | Device Default State Configuration | | |
| Trusted Certificate Authorities 802.1X * On Demand Overwrite | Atzess Setub Wizerd | Hut Configured | Configure- |
| | | | Back Training |
| | | | |

| Internet Services | XEROX WorkCentre 5675 | 🔛 allmin - Lagand Huma Salas Sita Hay Holp |
|--|---|--|
| Matus John Print Scan | Properties Support | |
| Properties Configuration Overview Description "General Setup F Connectivity | Authentication Londouration > CAC/PIV Setup | |
| * hervices * Accounting * Security User Data Encrypton | Smart Card Timeaut System Inactivity until smart card user is lagged off D (Montes (1 - 120)) | |
| Considering Considering Considering Considering Considering Available Oppal Certificate Nacassent Trusted Certificate Authorities 82.2.X **On Demand Overwrite | Denning Cantraliter IESE Certificate Validation | |
| | Damain Controller | |

Note: At the completion of

configuration of CAC, you can return to this screen and Configure the Device Access permissions if desired. Please refer to the system administrator guides appropriate for your product.

5. Domain Controller validation

If your site does not register the DC with OCSP:

- a. Uncheck all three **Domain Controller OCSP Certificate Validation** boxes and add the required Domain Controller.
- b. Select Save. Go back and add other Domain Controllers as required.

If you wish to validate the DC against OCSP before validation of the user:

- a. Check the box for Validate Before CAC/PIV Authentication.
- b. Enter the OCSP Server Service URL details.

Note: Depending on your environment, these details may be case sensitive.

If you wish to validate the DC against OCSP after validation of the user:

- a. Check the box for Validate after CAC/PIV User Authentication.
- b. Enter the OCSP Server Service URL details.
- c. If you wish to validate the DC certificate retrieved as part of the user authentication process against the one stored during installation, check the box for Domain Controller Signature must match uploaded Domain Controller Certificate.



- 6. Enter the **Domain Controller** details for the authentication server.
 - a. Determine how many Domain Controllers used in your environment need to be accessed from the particular device.
 - b. Identify the order the Domain Controllers should be interrogated when users present their card for authentication. The Domain Controller which services



most of your users should be first followed by less popular Domain Controllers.

c. Enter the controllers in the preferred search order.

Note: The search order can be modified at a later date.

- d. Select Add.
- e. Ensure the *Domain Controller Type* is configured correctly for your authentication environment.
- f. Enter the *IP Address* or enter the *Domain Controller Host Name* (this must be the fully qualified Host Name).
- g. Ensure *Port 88* is selected unless your Kerberos Port is different.
- h. Enter the *Domain Name* (this must be the fully qualified Domain Name).
- i. Select Save.

If you selected the option that the Domain Controller Signature must match the uploaded Domain Controller Certificate, then a field will be presented to enter that certificate. This field will be missing if it is not required to upload the Domain Controller Certificate.

j. At the *Domain Controller Certificate* option select **Add** and browse to the Domain Controller Certificate.

Note: If you are unable to obtain the required certificates, refer to Retrieving the Certificate from a Domain Controller or OCSP Server on page 39.

k. Select the Certificate then select Upload Domain Controller Certificate.

| Status | Jobs | Print | Scan | Properties | Support | |
|---|--|--|-----------|---|--|--|
| Propert | es | | | Authenticat | ion Configura | ion |
| Configu Descript | ation Ove ion I Setup | rview | | 📄 Aut | henticati | on Configuration > CAC/PIV Setup > Add Domain |
| * Service | tivity e | | | Add Dom | ain Controll | er |
| Securit User D Auther IP Filte Audit L Machin Ianageme Truster On De | Y ata Encrys titation G og e Digital C nt J Certifica mand Ov | ation onfiguratio Certificate te Authorit erwrite | n ties | Domain (Windo DiPv4 / DiPv6 / Host f | ontroller T ws Based Do Address Address Jame | pe nain Controller IP Address: Port 111 , 222 , 33 , 44 |
| | | | | Domain domain Domain (| controller C | rtificate |
| | | | | Add | | |

👪 admin - Logout | H

If the Domain Controller certificate is not available, the certificate that was used to issue the Domain Controller certificate can be uploaded instead.

The Domain Controller certificate, or its issuing certificate is needed by the device to validate the interactions between the device and the domain controller.

m. Repeat the process to enter the

I. Select Save.



XEROX WorkCentre 5030

If an error is made, select the Domain Controller from the list, and make any corrections. Select Edit.

Internet Services

- n
- Make any changes, then Select Save. 0

Note: To change the Domain Controller search order, select the controller and use the up and down arrows on the right side of the screen to promote or demote the controller order.

7. Upload certificates

> Note: These steps are Read Only if using any of the OCSP Certificate Validation options.

Load the DC root and intermediate certificates and the OCSP root and intermediate certificates:

- Select the Link to Security > α. Trusted Certificate Authorities Page option or select Trusted Certificate Authorities from the menu.
- b. At the Trusted Certificates Authorities screen, select Add.
- Browse to the previously c. retrieved certificates and add them one at a time.
- Select the certificate then select d. the Upload Certificate Authority button to add each one.
- Repeat the process until all e. certificates are installed.
- f. Select Close.

| Internet Services | XEROX Wo | rkCentre 5 | 030 | |
|---|--|---|--|----------------------|
| Status Jobs Print Scan | Properties | Support | | - |
| Properties Configuration Overview Description 7 Cennectivity 9 Services 9 Security User Data Encryption Authentocoton Configuration 19 Filtering Audit Log Machine Digital Certificate Nangement Trusted Certificate Authorities • On Demand Overwrite | Authenticat Authenticat Smart Ca System I 5 Domain (V valid V valid Domain (uploadec V fand C trutter (Domain (uploadec C trutter (Domain (uploadec C trutter (Domain (Later (| ion Configura henticati ard Timeout nactivity un Minutes (1 - 1 controller Ol ate before C ate after CA controller Si Domain Co a ertificate Auth controller # Delete cac.local | tien on Configuration > CAC/PIV Setup til smart card user is logged off 20) SP Certificate Validation AC/PIV User Authentication C/PIV User Authentication gnature must match northes Page | Service http://oc |



- 8. Check the Proxy Server details are configured
 - a. If required by your network environment, ensure the Proxy Server details have been configured.
 - b. Select the **Properties** tab, then **Connectivity**, **Protocols** and **Proxy Server** and enter the details.
 - c. Select Apply.
 - d. The *Smart Card* settings are now configured.

The Smart Card settings are now configured. You are now ready to install the Smart Card hardware using the instructions starting on page 26.

| Status Jobs Print Sc | an | Properties | Supp | port | _ | _ | | _ | | _ | _ | |
|---------------------------------------|----|------------|------------|--------------|----------------|-------------|--------|-------------|-----|-------------|---|------|
| Properties | | Proxy | Serve | r | | | | | | | | |
| Configuration Overview Description | | HTTP P | oxy Ser | ver | | | | | | | | |
| General Setup | | | | | | | | | | | | |
| -Connectivity | | 🗹 Enat | led | | | | | | | | | |
| *Protocols | | (a) 10.04 | Address | | | | IP Add | fress: Port | | | | |
| AppleTalk | | 0 10.00 | Address | | | | 0 | 0 | 1 | | | 9090 |
| IP (Internet Protocol) | | O How | Harress | | | | 0 | | 1.6 | | | |
| SUP | | C Host | Norrie | | | | | | | | | |
| SNMP | | | | | | | | | | | | |
| Microsoft Networking | | | | | | | | | - E | Default All | | Unc |
| LPR/LPD | | | | | | | | | | | | _ |
| SMTP Server | | Note | | | | | | | | | | |
| LDAP | | These se | ttings wil | I be used fo | r the followin | g features: | | | | | | |
| POP3 Setup | | | | | | | | | | | | |
| Proxy Server | | • 5 | Mart eSo | lutions Setu | 2 | | | | | | | |
| NTP | _ | • <u>H</u> | TTP(S) F | le Destinati | 105 | | | | | | | |
| P Services | _ | • H | TTP(S) T | emplate Por | 4 | | | | | | | |
| (secondy | | | | | | | | | | | | |
| | | | | | | | | | | | | |

| Internet Services | XEROX WorkCentre 5050 | 🔏 admin - Logest His | ne Index file Rap |
|--|--------------------------------------|--|-----------------------|
| Status Jobs Print Scan | Properties Support | | |
| Properties Configuration Overview Description | Authentication Configuration | | |
| ▼General Setup | Current Configuration | | |
| Coofiguration Cloning Image Settings Internationalization • Alert Notification • Nachine Software | Authentication | Device User Interface Authentication CAC/PIV | Edit Metho |
| *Connectivity *Physical Connections | Device System Administrator Password | | M |
| AppleTalk NetWare SP (Internet Protocol) SLP SNAP | Device User Interface Authentication | Configured | |

Xerox WorkCentre 5735/5740/5755/5765/5775/5790 (System Software 06x.131.xxx.xxxx):

- 1. At the WorkCentre, press the **Machine Status** button on the control panel.
- 2. Select the **Tools** tab.
- 3. Enter the appropriate User ID and Password to access Tools.

Note: The default user name and password are: admin and 1111.

- 4. Select Service Settings.
- 5. Select Optional Services.
- 6. Select Smart Card.
- 7. Using the keypad, enter the Feature Enablement Key included in the *Smart Card* Enablement Kit, and press **Enter**.

Configuring Authentication

- 1. In CentreWare Internet Services, click **Properties > Security > Authentication**.
- 2. Click Setup.
- 3. Click Edit.
- Under Authentication method on the machine's touch interface, select Smart Cards.
- 5. You can configure an alternate authentication method to allow users to access the printer without a *Smart Card*. Under *Alternate authentication method on the machine's touch interface*, select **User Name / Password Validated Remotely on the Network**.

| itemet Services | XEROX WorkCentre | 5745 | |
|---|---------------------|--|-------------------------------|
| Status Joke Print Scan | Address flack Prope | riles Superio | |
| Properties Configuration Overview Description General Setup | Authentica | intraction.Nethods | |
| Connectivity | Enablement | | |
| Accounting | (CTA) (0) | Authentication method on the machine's touch inter | face (Touch UI) |
| Security Secure Print Encryption | | Smart Cards | • |
| Authentication Entrop Tools & Pesture Access | | Supported Smart Cards | |
| DF Filtering | | Alternate authentication method on the machine's to | such interface (Touch III) |
| Audit Log Security Certificates IPaac | | Disabled | • |
| 002-1X System Timeout On Demand Overwrite Display Network Settings | | Who result I use this feature? | |
| | | Authentication method on the machine's web over in | steelere (Web UI) |
| | • | User Name / Password Validated Locally on the Xerox Ma | chine + |
| | - | Authorization information is stored | |
| | | Locally on the Xerox Machine (Internal Database) + | |
| | | Personalize the machine's touch interface | |
| | | Automatically retrieve the following information for the Nome directory for the "Scan to Home" service. E-mail address for the 'E-mail' service. | authenticated user from LDAP(|
| | _ | | Search Second Second |

6. Specify a method for the printer to authenticate users who access CentreWare Internet Services from their c

CentreWare Internet Services from their computer. Under Authentication method on the machine's web user interface, select User Name / Password Validated Locally on the Xerox Machine or User Name / Password Validated Remotely on the Network.

- 7. Under Authorization information is stored:, select Locally on the Xerox Machine, or Remotely on the Network.
- 8. Click Save.
- 9. A list of configuration settings appears at the bottom of the Authentication Setup page.
- 10. Click Edit to configure any settings that are marked in red text as Required; Not Configured.

Configuring Domain Controller Settings

 In the related services table on the Authentication Setup page, click Edit... on the Domain Controller(s) row. The domain certificate on a Smart Card of a user must be validated on the domain controller server before they can access the printer.

| Internet Services | Address flook Properties Support | |
|--|---|-------------------------------------|
| Properties Configuration Overview Decomption Connectivity Konnectivity | Arthentication & Arthenization Intra-Immun Centrolled al | |
| *Services *Accessing *Security *Security *Accession *Accessio | Daman Catholum Type 20 United and Daman Catholar 20 Den Address 20 Net Andress 20 Net Network | 17 Address Fort 0 .0 .0 .0 .0 .0 |
| Display Network Settings | J | Cancel Ser |

- 2. Click Add Domain Controller.
- 3. Under Domain Controller Type, select Windows Based Domain Controller if you are using one.
- 4. Type the domain controller server address information.
- 5. Click Save to apply the new settings or Cancel to return to the previous screen.
- 6. If you have added more that one domain controller server, you can prioritize the alternate servers.
- 7. Click Change Domain Priority.
 - a. On the Change Domain Priority page, select a domain controller in the list.
 - b. Click the **Up** Arrow or **Down** Arrow to change the search priority of the server.
 - c. Click Close.

- 8. To configure NTP settings, under *Action*, click **Edit**... next to NTP. The domain controller time and the time set on the printer must be synchronized. Xerox recommends that you enable NTP to ensure time synchronization.
- 9. Click **Close** to return to the *Authentication Setup* page.

Configuring OCSP Validation Server Settings

If you have an OCSP server, or an OCSP certificate validation service, you can configure the printer to validate certificates installed on the domain controller.

reware*

XEROX WorkCentre 5745

- 1. On the *Authentication Setup* page, under *Action*, click **Edit** next to Certificate Validation.
- 2. Select a validation method and click **Next**.
- 3. On the *Required Settings* page, type the URL of the OCSP server.
- 4. To ensure that the printer can communicate with the OCSP server and the domain controller, configure your proxy server settings if necessary.

| perties Validation Detinor | |
|---|---|
| Maj unita Oranita mala Statu mark Statu | Valuate the vertilizate returned from the domain evolvator evolves and the CSSP serves. # to © Yes Why model 1 use this fasture: |
| Ser Jafenengino Catalase Pritanog udi Log Telanog udi Log udi Log Negen Tenesul splay Tetenok Jettings | Validate the domain controller contribute starts on the Xeree machine against OOP antwork. \bigcirc |
| | Validate the s-suit encryption certificate from the smart card easiest the COS encryption certificate from the smart card # for 0 res Who would Least the featurest |
| ₩ → © | Validate domain controller contribute wheread by the domain started on the Varian evolution, much controller contribute where do the Varian evolution, and the variance in the Varian evolution of the Varian evolution of the Varian evolution of the Varian evolution of the Variance of the Variance War and J and the formers? |

- 5. Click the appropriate link to install the root CA certificates for the OCSP server and your domain controller.
- 6. Click **Save** to apply the new settings and return to the *Authentication Setup* page. Click **Cancel** to return to the *Authentication Setup* page.

Setting the Inactive Time Limit

- In the related services table on the Authentication Setup page, click Edit... on the Smart Card Inactivity Timer row.
- Specify the maximum amount of time before a user is automatically logged out. Type the time in minutes.

| nternet Services | XEROX WorkCentre 5745 | |
|--|--|--|
| Status Jobs Print Scan | Address Book Properties Support | |
| Properties | Authentication Configuration | |
| Configuration Overview Description | Smart Card Inactivity Timer | |
| +Connectivity | | |
| Services | Smart Card Inactivity Timer | |
| Accounting Secure Print Secure Print Plot 140-2 User Osta Encryption Authentication Secure Tools & Frature Access Tools & Frature Access | Plinotes 5 (1 - 120) | If logget in users do not interest with the medine's Touch User interfacility for interactional within the true disclock, setting all to reveal to the set of the s |
| User Information Database P Fibering | Note | |
| Audit Log Security Certificates IPsec 802.1X System Timeout Durate Materials Sattings | The Smart Card Inactivity Timer overrides the Review Evidem Timer settings. | such user interface System Timer after the user auccessfully logs in. |

 Click Save to apply the new settings and return to the Authentication Setup page. Click Cancel to return to the Authentication Setup page.

Acquiring Logged in User's E-Mail Address

This feature allows the System Administrator to set where the device acquires the logged in user's email address from when populating the e-mail *From:* field.

Using the default **Auto** setting, the device checks the *Smart Card* for the user's e-mail address information. If the information is not available from the card, the device checks the LDAP server. If the information is not available from the LDAP server, the device uses the default e-mail address to populate the field.

If required, the System Administrator can change the setting to obtain the user's e-mail address from the *Smart Card* only, or from the *Network Address Book (LDAP)* only.

roperties

T

-mail Encryption / Signing

imart Card Inactivity Timer

couiring Logged in User's E-n

Certificate Validation

 In the related services table on the Authentication Setup page, click Edit... on the Acquiring Logged in User's E-mail Address row.

- Select the option required for obtaining the logged in user's e-mail address:
 - Auto
 - Only Smart Card
 - Only Network Address Book (LDAP)

If **Only Network Address Book** (LDAP) is selected, configure the *Server Configuration* and *Feature Enablement* settings required.

| | Tools and Peature Access (Lock / Unlock) | Authorization | Contional; Configured | _ | | |
|---|--|---|-------------------------------|-------|--|--|
| | Graphic Key | | | | | |
| | | | | | | |
| | | | | | | |
| C | | | | | | |
| E-mail Setu | ip. | | | | | |
| Policies | | | | | | |
| Acquire logged in u | ser's e-mail address from | Auto | | | | |
| Auto | | Procedure to acquire the | logged in user's e-mail addre | 551 | | |
| O Only Smart Card | | 1) Smart Card 2) Theo Network Address Book (LDAR) | | | | |
| O Only Network Address Book (LDAP) | | Use system's default 'From' field value; printer13@opdu-dev.net | | | | |
| | | | | - | | |
| | | | | | | |
| | | | | | | |
| Related Configurati | on Settings | | | | | |
| Related Configurati | on Settings | | | | | |
| Related Configuration | on Settings | | | | | |
| Related Configurati ierver Configuration Setting | on Settings | Status | | ction | | |
| Related Configuration Setting Network Address Bo | on Settings | Status | A | ction | | |
| Related Configurati ierver Configuration Setting Network Address Bo | on Settings ok (LDAP) | Status | | ction | | |
| Related Configurati lerver Configuration Setting Network Address Bo reature Enablement | on Settings ok (LDAP) | Status | | ction | | |
| Related Configurati erver Configuration Setting Network Address Bo eature Enablement Setting | an Settings ek (LDAP) | Status Profigured | Ac | ction | | |

User Name / Password Validated Remotely on the Network

s on the ma

Authentication (Touch UI)

Authentication (Touch UI)

Authentication (Touch UIT)

Alternate Authentication (Tou UI): Authentication (Web UI) R

- Opti

and Oats

3. Click **Save** to apply the new settings and return to the *Authentication Setup* page. Click **Cancel** to return to the *Authentication Setup* page.

Configuring E-mail Encryption and Signing Settings

- In the related services table on the Authentication Setup page, click Edit... on the E-mail Encryption/Signing row.
- 2. To enable E-mail Encryption, under *E-mail Encryption Enablement*, select an option:
 - Always On; Not editable by user: Restrict users from turning E-mail Encryption on or off at the control panel.
 - Editable by user: Allow users to turn E-mail Encryption on or off at the control panel.

| entreware" nternet Services | XEROX WorkCentre 5745 | 🙏 admin - Lagent Hume Sules Site Hap Help |
|--|--|--|
| Statue Joke Print Scan | Address Book Properties Support | |
| Properties Configuration Overview Description PGeneral Setup PCeneral Setup | Authentication Configuration | |
| Accounting *Security Secure Print | | When the "Broryption & Eigning" feature is on, the feature is located within the E-mail service on the "E-mail Options" tab within the machine's fouch interface. |
| *Encryption *Authentication Betup Tools & Feature Access | | Flice, the settings balance alive you to prest or restrict the vallop user form modeling the encryption and signing default values within the machine's touch interface. |
| IP Financy Audit Log Security CethTcates Effect D02,1X Bystem Toresut Display Network Settings | E-mail Excryption Enablement Corr Corr Education Service Corr Education Service Excryption Algorithm Excryption Algorithm Excryption Algorithm Excryption Algorithm Corr Education Algorithm Excryption Corr Education Corr Educa | E-mail Excerption Default © Of On |
| | E-mail Eigning Enablement # Off Oni: Editable by user Digning Heah SHAL | E-mail Signing Defnuh © Off © On |
| | | Canoel Save |

3. If you select Editable by user, select the default setting for users at the control panel. Under *E-mail Encryption Default*, select **On** or **Off**.

- 4. Under *Encryption Algorithm*, select one of the following encryption methods:
 - 3DES
 - AES128
 - AES192
 - AES256
- 5. To enable E-mail Signing, under *E-mail Signing Enablement*, select an option:
 - Always On; Not editable by user: Restrict users from turning E-mail Signing on or off at the control panel.
 - Editable by user: Allow users to turn E-mail Signing on or off at the control panel.
- 6. If you select Editable by user, specify the default setting for users at the control panel. Under *E-mail Signing Default*, select **On** or **Off**.
- 7. Click **Save** to apply the new settings and return to the *Authentication Setup* page. Click **Cancel** to return to the *Authentication Setup* page.

The *Smart Card* settings are now configured. You are now ready to install the *Smart Card* hardware using the instructions starting on the next page.

Hardware Installation

Install the card reader device using the following instructions.

1. Unpack the Smart Card Enablement Kit

The kit contains the following items:

- Xerox Smart Card Enablement Guide (1).
- Four Dual Lock Fastener pads (Velcro) (2).
- Three Cable Ties (3).
- One Ferrite Bead (4).

Ensure you have read the licence agreement and agree to the terms and conditions specified prior to installation.



- 2. Locate the card reader device being installed
 - There are four types of card reader available, one upright model or three slimline models.
 - Locate the device being installed and ensure it has been configured.

Note: The System Administrator should configure the cards prior to the card reader being installed on the machine.



Installation

3. Attach the ferrite bead to the reader cable.

Note: The ferrite bead should be clipped onto the cable directly behind the connector.



- 4. Attach the fasteners to the card reader device
 - Fasteners have been provided to secure the card reader to the Xerox device.
 - Peel back the fastener backing strip.
 - Position the fastener on the under-side of the card reader, as shown.
 - Repeat for each of the fasteners supplied.



5. Remove the fastener backing strips

When all the fasteners have been attached to the card reader, remove the backing strips on each of the fasteners.



- 6. Place the card reader on the Xerox device
 - Gently place the card reader on the device (do not fix in place at this point).
 - Position the card reader in a suitable location, ensure it does not obstruct the opening of the document handler side cover.
 - Check the cable has sufficient length to connect to the rear of the network controller.
 - Once it is in a suitable location, press firmly on the card reader to fix it in place.



- 7. Connect the card reader to the Xerox device
 - Insert the USB connection into the slot provided on the rear of the network controller.
 - Use the cable ties provided to ensure the cabling is neat and tidy.



The hardware installation is now complete.

- 8. Confirm the installation
 - When the card reader and the software has been installed and configured, the *Card Reader Detected* screen displays on the Xerox WorkCentre local user interface.
 - Select OK.

Smart Card is now ready for use.

Note: If the card reader is not detected, refer to Troubleshooting Tips on page 37 for information.

Using the Smart Card

Once the *Smart Card* has been enabled, each user must insert a valid card and enter their Personal Identification Number (PIN) on the touch screen. When a user has finished using the Xerox WorkCentre, they are then required to remove their card from the card reader to end the session. For instances where a user forgets to remove their card, the machine will end the session automatically after a specified period of inactivity.

Follow the instructions below to use the Smart Card:

- 1. The *Authentication Required* window may display on the touch screen, depending on your machine configuration.
- 2. Insert your card into the card reader.
- Use the touch screen and numeric keypad to enter your PIN and then select Enter. If the card and PIN are authenticated, access is granted. If the access attempt fails, refer to Troubleshooting Tips on page 37.
- 4. Complete the job.
- 5. To end the session, remove your card from the card reader.

The current session is terminated and the Authentication Required window is displayed.

Troubleshooting



For optimal performance from your card reader, ensure the following guidelines are followed:

- The Card Reader is only compatible with network connected products.
- Ensure the Card Reader is plugged into the Network Controller. Refer to Connect the card reader to the Xerox device on page 32 for instructions.
- Do not position the Card Reader in direct sunlight or near a heat source such as a radiator.
- Ensure the Card Reader does not get contaminated with dust and debris.

Fault Clearance

When a fault occurs, a message displays on the User Interface which provides information relating to the fault. If a fault cannot be resolved by following the instructions provided, refer to Troubleshooting Tips on page 37.

If the problem persists, identify whether it is related to the card reader device or the Xerox device.

- For problems with the card reader device, contact the manufacturer for further assistance.
- For problems relating to the Xerox device, contact the Xerox Welcome and Support Center. The Welcome and Support Center will want to know the nature of the problem, the Machine Serial number, the fault code (if any) plus the name and location of your company.
 Contact Xerox using the numbers 1-800-ASK-XEROX or 1-800-275-9376.

Locating the Serial Number

- 1. Press the Machine Status 🔁 button on the control panel.
- 2. Information about the machine is displayed. If necessary, select **Machine Details** to display the *Customer Support Number* for the *Welcome and Support Centre* and the *Machine Serial Number*.

The serial number can also be found on a label inside the front door.

Troubleshooting Tips

The table below provides a list of problems and the possible cause and a recommended solution.

If you experience a problem during the installation process please refer to the During Installation problem solving table below.

If you have successfully installed the *Smart Card* solution but are now experiencing problems, refer to After Installation: on page 38.

During Installation:

| Problem | Possible Cause | Solution |
|--|---|--|
| Card reader is installed but no message displays on the User Interface | • Card reader is faulty. | Try a different card reader.Contact the System Administrator. |
| | • Card reader connection is faulty. | Check the cable is plugged in correctly. Refer to Hardware Installation on page 26 for instructions. Unplug the card reader cable then plug back in. Plug the card reader into a different USB port. |
| | • Card reader is not compatible. | • Check that the card reader is on the list of compatible devices, refer to Supported Card Types on page 7. |
| | • <i>Smart Card</i> access is not enabled on the machine. | • Enable CAC through the <i>Properties</i> set up screens using Internet Services, refer to Configuring the Smart Card on page 13. |

After Installation:

| Problem | Possible Cause | Solution |
|---|---|--|
| Authentication failures | Incorrect PIN has been entered. | • Retry entering the correct PIN. If problem persists, contact the System Administrator for advice. |
| | Card is locked due to too many failed PIN attempts. | • Contact Registration Authority to reload or to get a new card. |
| | Unable to find identity certificate. | |
| | Identity certificate has been revoked. | |
| | Authentication with Domain Controller Failed. | • Check network cable is firmly connected. |
| | Unable to validate server certificate. | Contact the System Administrator. |
| | • Smart Card Authentication System Failed. | |
| | Authentication Failed. | |
| | • System Administrator has not selected All Features or Scanning Service Only. | Contact the System Administrator. |
| Time for date mismatch error | • There is a mismatch between the time and date setting on the Xerox WorkCentre and the authentication server time or date setting. | Verify that Network Time Protocol is properly set up. Verify that GMT offset is correct for your region, refer to Configure the date and time to update automatically on page 13. Verify that GMT offset is correct for Daylight Savings Time. Contact your System Administrator. |
| Cannot see the Internet Services web page after software upgrade | • IP Address incorrect or has been reset. | Check the IP Address printed on the configuration report. Ensure the DHCP settings match your site settings. To print a configuration report at the Xerox WorkCentre. |



Retrieving the Certificate from a Domain Controller or OCSP Server

1. Access the Domain Controller using a web browser using the following syntax: https://IP Address of the Domain Controller:636

For example: *https://111.222.33.44:636* where *111.222.33.44* is the IP address of the appropriate server. A *Security Alert* warning window is displayed, similar to the one shown.

2. Click on View Certificate to proceed.

If the window does not display, double click on the padlock icon in the lower right hand corner of your browser window.

| Securit | Alert 🛛 |
|---------|--|
| ß | Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate. |
| | The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority. |
| | The security certificate date is valid. |
| | The name on the security certificate is invalid or does not match the name of the site |
| | Do you want to proceed? |
| | Yes No View Certificate |

The Certification Information window is displayed.

| Certificate ? 🔀 | |
|--|--|
| General Details Certification Path | |
| Certificate Information | |
| This certificate cannot be verified up to a trusted certification authority. | |
| | |
| | |
| Issued to: ICE-T.dssc.mc.xerox.com | |
| Issued by: Xerox Generic Certificate Authority | |
| Valid from 4/23/2008 to 9/8/2035 | |
| | |
| Install Certificate Issuer Statement | |

3. Select the **Details** tab.

Record the name of the *Certificate Authority (CA)* that issued this certificate, the "Issuer".

A certificate from this CA will be required during *Smart Card* setup.

4. Select the **Copy to File** button.

| Certificate | ? 🛛 |
|--|---|
| General Details Certification Path |] |
| Show: <a> | ~ |
| Field | Value |
| Version Serial number Signature algorithm Issuer Valid from Valid from Subject Public key | V3 O0 as 6e 94 ca mdSR5A Xerox Corporation, Fairport, N Wednesday, April 23, 2008 11 Saturday, September 08, 203 xerox, crmt, me@here, us, RSA (1024 Bits) |
| Ec | lit Properties |

The Certification Export Wizard is displayed.

5. Select Next.

| 6. | Select Base-64 encoded X.509 | (.CER). |
|----|------------------------------|---------|
|----|------------------------------|---------|

7. Select Next.

| Certificate Export Wizard | X |
|---------------------------|---|
| | Welcome to the Certificate Export Wizard |
| | < Back Next > Cancel |

| Certificate Export Wizard | | | |
|--|--|--|--|
| Export File Format Certificates can be exported in a variety of file formats. | | | |
| Select the format you want to use: | | | |
| O DER encoded binary X.509 (.CER) | | | |
| Base-64 encoded X.509 (.CER) | | | |
| Cryptographic Message Syntax Standard - PKCS #7 Certificates (,P7B) | | | |
| Include all certificates in the certification path if possible | | | |
| Personal Information Exchange - PKCS #12 (.PFX) | | | |
| Include all certificates in the certification path if possible | | | |
| Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above) | | | |
| Delete the private key if the export is successful | | | |
| | | | |
| < Back Next > Cancel | | | |

8. Select Browse.

Browse to a directory to save the Certificate.

- 9. Enter a filename for the *Certificate* and select **Save**.
- 10. Select Next.

| rti | ficate Export Wizard |
|-----|--|
| i | e to Export Specify the name of the file you want to export |
| | File name: |
| | C:_Certificates\My Domain Controller Certificate.cer Browse |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | < Back Next > Can |

11. Select Finish.

The *Certificate* is retrieved from the server and saved in the selected directory.

A pop-up message will confirm that the *Certificate* has been successfully saved.

Once saved the *Certificate* can be loaded onto the device.

This process can be repeated to retrieve the *Certificates* from each of the required servers.

| Certificate Export Wizard | | | | |
|---------------------------|--|--|--|--|
| | Completing the Certificate Export Wizard You have successfully completed the Certificate Export wizard. You have specified the following settings: | | | |
| | File Name C:/WO Export Keys No Include al certificates in the certification path No File Format Base6* | | | |
| | < Back Finish Cancel | | | |

Retrieving the Certificate from a Domain Controller or OCSP Server

B

Determining the Domain in which your Card is Registered

- 1. From your PC, click the **Start** menu and right click on **My Computer**.
- From the drop down list, select Properties.
 When the System Properties window opens, click on the Computer Name tab.
 Beneath the Full Computer name is the Domain Name.
- 3. Copy and paste the *Domain Name* directly into the CAC setup page on the Internet Services user interface.

Refer to Configuring the Smart Card on page 13 for instructions.

4. Select **Cancel** to close the *System Properties* window.