PKI-Enabled MFP

Pre-Installation Guide

Version 2.0.0

www.lexmark.com

Edition: April 2008

The following paragraph does not apply to any country where such provisions are inconsistent with local law: LEXMARK INTERNATIONAL, INC., PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in later editions. Improvements or changes in the products or the programs described may be made at any time.

Comments about this publication may be addressed to Lexmark International, Inc., Department F95/032-2, 740 West New Circle Road, Lexington, Kentucky 40550, U.S.A. In the United Kingdom and Eire, send to Lexmark International Ltd., Marketing and Services Department, Westhorpe House, Westhorpe, Marlow Bucks SL7 3RQ. Lexmark may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you. Kingdom and Eire, call +44 (0)8704 440 044. In other countries, contact your point of purchase.

References in this publication to products, programs, or services do not imply that the manufacturer intends to make these available in all countries in which it operates. Any reference to a product, program or service is not intended to state or imply that only that product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any existing intellectual property right may be used instead. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by the manufacturer, are the user's responsibility.

ImageQuick, Optra, Lexmark, and Lexmark with diamond design are trademarks of Lexmark International, Inc. registered in the United States and/or other countries.

Other trademarks are the property of their respective owners.

UNITED STATES GOVERNMENT RIGHTS
This software and any accompanying documentation provided under this agreement are commercial computer software and documentation developed exclusively at private expense.

Table of Contents

1 Background Information

1.1 Document Overview

This document should be used as a checklist or questionnaire and completed prior to the installation of a Lexmark PKI-Enabled MFP. The intent is to gather all the information necessary to configure the PKI applications on the Multi-Function Printer (MFP) once it has been installed. The data collected using this pre-installation guide will be needed to complete the installation instructions in the *Lexmark PKI-Enabled MFP Installation and Configuration Guide*.

If you have questions about the information requested in this pre-installation guide, you may:

- Call 1-888-LXK-SOLV and choose option 4
- Send an email to lxksolv@lexmark.com

1.2 PKI/AD Solution

The Lexmark PKI/AD Solution allows a user to authenticate against Active Directory using a SmartCard (such as the Department of Defense Common Access Card) or a userid and password both using the Public Key Infrastructure. The complete solution is composed of several applications:

- PKI/AD Authentication – Main application; it must be installed and running for all the other PKI applications to function. It provides the login screen and authentication mechanism. It also supports the user authorization support for device and/or individual device functions.

- PKI/AD Standard Applications – Provides user authorization support for the standard Copy, Fax, and FTP functions on the device.

- PKI/AD Email – Provides user authorization support and enhanced email functionality; this includes greater control over the standard email interface, digital signing and encryption of emails, and setting of the "from" address to that of the authenticated user.

- PKI/AD Scan To Network – Provides the ability to scan to a user's home directory or to other pre-defined fileshares. The fileshare names can be built dynamically using information about the authencticated user from AD. User authorization can be used to limit access to this function or to individual fileshares.

- PKI/AD Print Release – This application is an extended feature of the PKI/AD solution and must be purchased separately; it requires the use of the Lexmark Document Solutions Server software. It allows users to print to a special print queue; the jobs are held by the server until the user releases them at the MFP. Jobs can be automatically deleted if not released within a certain amount of time. Contact your Lexmark Sales Representative for more information.

1.3 SmartCard Contents

The SmartCard contains at least two certificates:

- Identity
- Email

The identity certificate is not used by this application.

The Email certificate is used by this application. The certificate contains several important pieces of information:

- *Smart Card Logon Enhanced Key Usage* – This flag indicates the certificate can be used for logging onto a Windows system. See Microsoft's documentation (http://support.microsoft.com/kb/281245) for this requirement.

- User Configuration Information
  - *Universal Principal Name (UPN) and EDI-PI* - The UPN provides a standard identifier used throughout the organization. The standard format for the UPN is:

    <principal name>@<common domain name>

    For a military CAC card, the UPN would be something like:

    12345678@mil

    The *mil* is the DoD's common domain name.

    The *12345678* is the *EDI-PI*. The EDI-PI can be used as an identifier independently when separated from the *mil* domain.

  - *Email Address* – The user's Email address:

    joe.smith@branch.us.mil

    This information is also referred to as the *RFC822* name.

  - *Subject Name* – The user's Distinguished Name on the DoD's PKI system:

    CN=SMITH.JOE.12345678, OU=Contractor, OU=PKI, OU=DoD, O=U.S. Government, C=US

    This subject name will typically be different than the subject name used in the IT systems for an individual branch or command organization.

1.4 Network Port Access

The MFP will need to access the network via several ports. The following table lists the default ports needed based on the features that are used.

Port	Protocol	Required by which Feature
25	SMTP	Scan to Email
53	DNS	DNS Lookups
80	Web	Web Configuration / OCSP Validation
88	Kerberos	Active Directory Authentication
389	LDAP (non-SSL)	Email Address / Home Directory LDAP Lookup
445	Windows File Sharing	Scan To Network
636	LDAP (SSL)	Email Address / Home Directory LDAP Lookup

1.5 Key Contacts

Before proceeding, it may be helpful to identify the appropriate people that can be contacted for assistance in filling this document out and/or assisting during the initial install.

Administrator	Name	Phone
Active Directory		
Network		
Tumbleweed/OCSP		
Email		
Information Assurance Officer		

2 Basic Network Configuration

This section is used to help get the device setup on the network. Even if the device has already been added to the network, please complete this section so that this information can be used as needed.

2.1 IP Address

The device can be configured to acquire an IP Address via DHCP or a static IP Address can be assigned to it. Which method should be used?

□ DHCP □ Static IP Address

If using a static IP Address, the following information is needed:

1. The IP Address for the MFP needs to be assigned.
2. The IP Address of the Gateway: _______ . _______ . _______ . _______
3. The Netmask: _______ . _______ . _______ . _______

If the device has not or will not be connected to the network prior to the PKI installation, please make sure the appropriate people are available to assist in getting the device active on the network.

2.2 DNS and WINS Servers

In order for the device to function correctly on the network, it needs to be able to resolve DNS names. Please provide the IP Address for the following servers:

WINS Server: _______ . _______ . _______ . _______

Primary DNS Server: _______ . _______ . _______ . _______

Backup DNS Server (optional): _______ . _______ . _______ . _______

2.3 Time Server

In order for the device to authenticate, its time must be within five minutes of the domain controller. The time can be set manually on the device or it can get the time from a network time server. Should the time be set manually or via a time server?

□ Manual

□ Time Server
IP Address / Name: ____

2.4 Domain Names

In order for the device to resolve partially qualified DNS names, it needs to know the default domain and other domains that should be searched. For example, if the printer DNS name is "x.y.z", the domain would be "y.z". Provide the domain names for the following:

1. The printer will be assigned to a domain once it is on the network. What domain should it be assigned to?

   Printer Domain Name: ____

2. What domain is the Domain Controller assigned to?

   □ Same as Printer Domain Name

   □ Different Domain: ____

3. What domain is the LDAP Server assigned to?

   □ Same as Printer Domain Name

   □ Same as Domain Controller Domain Name

   □ Different Domain: ____

4. If scanning to the user's home directory will be enabled, the domain of the file servers hosting the directories will be needed. What is the domain of the file servers?

   □ Scan to Home Directory Will Not Be Enabled

   □ Same as Printer Domain Name

   □ Same as Domain Controller Domain Name

   □ Same as LDAP Server Domain Name

   □ Different Domain: ____

2.5 Default LDAP Configuration

Many of the PKI Applications utilize LDAP to perform queries that are used for getting other information about the authenticated user (such as home directory or email address) or for searching the address book when sending emails. The MFP supports a default LDAP configuration which is specified here. If some pieces of data need to be retrieved from other LDAP sources, those LDAP configurations can be specified at a later time.

1. IP address or name of a LDAP directory

   IP Address or Name: ____

2. Port used to communicate with the LDAP server. Typically this is 389 for non-SSL connections; 636 for SSL connections.

   Port: _____________

3. If SSL is required to communicate with the server, then the LDAP Server's SSL certificate will need to be installed on the device.

   □ SSL is not required

   □ SSL is required
   Certificate: Please have file ready at install time.

   If SSL is used, then the fully qualified domain name (instead of just the IP Address) needs to be used in item 1.

4. If using SSL, the LDAP Certification Validation method must be selected. If not using SSL, you can skip this step. The available validation methods are:

Never	Never – The certificate will not be requested or checked.
Allow	A certificate will be requested. If provided, it will be checked, but invalid certificates will be ignored.
Try	A certificate will be requested. If a certificate is provided, it must be valid. If a certificate is not provided, no error will occur.
Demand	A certificate will be requested. If the certificate is not provided, or is invalid, the LDAP connection will be terminated.

   Select the validation method:

   □ Never □ Allow

   □ Try □ Demand

5. Base name for search. This defines the section of the LDAP directory in which to start the search. The value is typically something like “dc=branch,dc=mil”.

   Search Base: ____

6. Search Timeout. The timeout in seconds after which the search is cancelled. Valid values are 5 to 300 seconds. The default of 30 seconds is recommended.

   Search Timeout: _________ seconds

7. Maximum Search Results. The maximum number of search results to be displayed to the user. Valid values are 5 to 500 results. The default value of 100 is recommended.

   Maximum Search Results: ___________

8. Access rights needed to access the LDAP directory. The device supports anonymous binding, the authenticated user’s credentials, or a service account using a Distinguished Name and password.

   ☐ Anonymous

   ☐ User’s Credentials (Cannot be used in Pin Only mode)

   ☐ Service Account
   Distinguished Name:____

   Password: _________ To be provided at installation _________

3 PKI/AD Authentication Configuration

This section describes the PKI-related login and logout decisions to make prior to installing the application on the device.

3.1 Login Screen

There are several options available for configuring what is displayed on the Login Screen. These options control which MFP functions are available without authenticating the user and the text and graphic displayed to the user.

3.1.1 Copy

The PKI Authentication application can allow copies to be made without logging onto the device. If the user is allowed to make copies without logging on to the device, check "Yes" below. If the user must log on to the device before making copies, check "No" below.

☐ Yes ☐ No

3.1.2 Fax

If Fax is enabled on the MFP, the PKI Authentication application can allow faxes to be sent without logging onto the device. If the user is allowed to send faxes without logging on to the device, check "Yes" below. If the user must log on to the device before sending faxes, check "No" below.

☐ Yes ☐ No

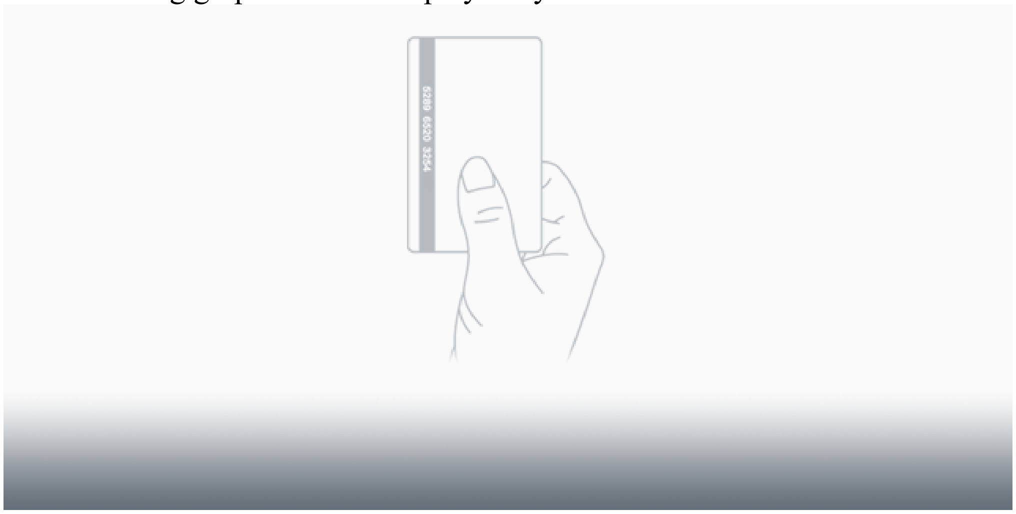
3.1.3 Login Text and Graphic

The login screen for the user contains text and a graphic prompting the user to insert their SmartCard to use the device. Optionally, it may contain the Copy and Fax buttons based on the answers above.

1. The login screen contains text directing the user on what needs to be done to use the device. The default text is based on whether the Copy or Fax buttons are available and the login types allowed. If alternate text is desired, please enter below.

Login Text: ____

2. The following graphic is also displayed by default.



If a different graphic is desired, it must be in GIF format and should be 640 pixels wide by 320 pixels high and no more than 40KB in size.

Alternate Graphic: Please have file ready at install time.

3.1.4 Login Type

The PKI Authenctication application can be configured to allow one of three login types:

Card Only	The user must insert his/her card to gain access to all device functions.
Manual Login Only	The user must enter his/her username and password to gain access to all device functions. In this mode, smart cards are not supported and the smart card reader is not attached to the MFP.
Card or Manual Login	The user can insert his/her card or username and password to gain access to all device functions.

Check the box below to indicate the desired logon method.

☐ Card Only

☐ Manual Login Only

☐ Card or Manual Login

3.1.5 Display MFP Info

The MFP can be configured to display various info in the upper left and right corners of the Welcome Screen. By default, the IP Address is displayed in the upper left and the current date/time is displayed in the upper right. (To change the info that is displayed, please consult the MFP's User Guide.) The PKI Authentication application can be configured to display that same information on the login screen. Do you want these items displayed on the login screen?

☐ Yes ☐ No

3.1.6 Display Printer Status

When there is an error or warning on the MFP, a “Status/Supplies” button is displayed on the welcome screen in the lower right corner. The PKI Authentication application can be configured to display the error or warning on the login screen. The user would still need to login to see the graphic or more detailed information, but this allows the basic warnings (Tray 1 Low) or errors (Load Paper Tray 1) to be seen or resolved without needing to login. Do you want the printer status available from the login screen?

☐ Yes ☐ No

3.2 User Authentication

The PKI Authentication application provides two methods for logging onto the device:

PIN Only	The user must enter his/her PIN number before obtaining access to the device; manual logins are not allowed.
Active Directory	The user must enter insert his/her card and enter the PIN number OR the user must enter his/her username and password. This information is sent to a Windows Domain Controller for validation. Once the information is authenticated the user is granted access to the device.

Check the box below to indicate the desired logon method.

☐ PIN Only ☐ Active Directory

3.2.1 PIN Only

No additional configuration information is needed for the *PIN Only* logon method. Using this mode, manual login is not supported and user’s certificate is not verified. The PKI Email application is the only other PKI application that can be used.

3.2.2 Active Directory

Windows Active Directory requires a SmartCard or Username/Password to be used for authentication. If using a SmartCard, the User Principal Name and certificate on the user’s card is sent to a Domain Controller to be validated. The Domain Controller sends a response back to the MFP; the response contains the Domain Controller’s certificate which the MFP must then validate. If using the manual login option, the username and password are sent to the Domain Controller to be validated.

In either case, the PKI Authentication application needs to validate the user against an Active Directory Domain Controller. The domain controller acts as a Kerberos Key Distribution Center (KDC) to validate the user.

1. IP address or name of the Active Directory Domain Controller to use for validation. Multiple domain controllers may be specified. List at least one below.

IP Address or Name: ____

IP Address or Name: ____

IP Address or Name: ____

2. Kerberos Realm (which is typically the Windows Domain Name). There is usually only one, but if more than one realm is used, a Kerberos Configuration File will need to be uploaded to the MFP. See section 7.3, *Kerberos Configuration File*, for information on generating this file.

   ☐ One Kerberos Realm: _______________________________________

   ☐ Multiple Kerberos Realms: Please have configuration file ready at install time.

3. For added security, the Kerberos and LDAP implementations used by the MFP perform reverse DNS lookups to verify IP Addresses. However, some networks have reverse DNS lookups disabled so this may need to be disabled. Are reverse DNS lookups disabled on the network that will be used by the MFP?

   ☐ Yes ☐ No

4. The KDC used for user authentication can also be set as the Default LDAP Server. This can allow for greater flexibility in case multiple KDCs are specified so that the LDAP server does not have to be set to only one of them. Do you want to set the default LDAP Server to be the KDC used for user authentication?

   ☐ Yes ☐ No

3.2.2.1 SmartCard Configuration

If SmartCard login is allowed, the PKI Authentication application needs to validate the response from the Domain Controller. It also must know the information to use from the card to lookup other data (such as home directory) about the user.

3.2.2.1.1 Response Validation

To validate the response from the Domain Controller is coming from a trusted source, the application must validate the certificate included in the Domain Controller's response. This validation can be done in one of four ways:

MFP Certificate Validation	The PKI Authentication Application gets the issuer of the certificate contained in the Domain Controller's response. In this case, the certificate of the Certificate Authority (CA) that issued the Domain Controller's certificate is considered trusted. So if the certificate of the CA that issued the certificate in the response is found installed on the MFP, the response is considered trusted and the logon proceeds. Otherwise, the logon will fail.

MFP Chain Validation	The PKI Authentication Application gets the certificate contained in the Domain Controller's response to build the complete certificate chain to a trusted Root CA. All certificates in this chain must have been previously installed on the MFP. If the chain can be successfully built, the response is considered trusted and the logon proceeds. If the chain cannot be built, the logon will fail.
OCSP Certificate Validation	The PKI Authentication Application gets the certificate contained in the Domain Controller's response and performs the same validation as in the *MFP Certificate Validation* mode. If that succeeds, it then uses an OCSP Responder/Repeater (such as Tumbleweed) to validate the Domain Controller certificate has not been revoked or otherwise marked as invalid. If that succeeds, the logon proceeds; otherwise, it fails.
OCSP Chain Validation	The PKI Authentication Application gets the certificate contained in the Domain Controller's response and performs the same validation as in the *MFP Chain Validation* mode. If that succeeds, it then uses an OCSP Responder/Repeater (such as Tumbleweed) to validate that none of the certificates in the certificate chain have been revoked or otherwise marked as invalid. If that succeeds for each certificate in the chain, the logon proceeds; otherwise, it fails.

The configuration information needed varies according to the Domain Controller Validation method selected. Check the box below to indicate the desired method.

☐ MFP Certificate Validation

☐ MFP Chain Validation

☐ OCSP Certificate Validation

☐ OCSP Chain Validation

If *MFP Certificate Validation* or *OCSP Certificate Validation* is chosen, the certificate of each CA that issued each Domain Controller certificate listed in item 1 in section 3.2.2 must be installed on the device. If *MFP Chain Validation* or *OCSP Chain Validation* is chosen, the certificate chain for each Domain Controller listed in item 1 in section 3.2.2 must be installed on the device.

Each certificate needs to be in PEM (Base64) format; see section 7.5, *Domain Controller Certificates*, for more information on generating the certificate file.

Certificate / Certificate Chain: Please have file ready at install time.

If one of the OCSP validation options is selected, the following information is needed about the OCSP Responder/Repeater to be used.

1. IP address or name of an OCSP Responder/Repeater along with the port being used. The default port is usually 80. Multiple responder/repeaters may be listed; they will be tried in order until a response is received.

   IP Address or Name: ___________________________________ Port: _______

   IP Address or Name: ___________________________________ Port: _______

   IP Address or Name: ___________________________________ Port: _______

2. IP address or name of the proxy server needed to access the OCSP Responder/Repeater along with the port being used. This is an optional setting and only needed if the OCSP Responder/Repeater is on the internet instead of the local intranet.

   IP Address or Name: ___________________________________ Port: _______

3. The maximum time in seconds that the MFP should wait for a connection to or response from the OCSP Responder/Repeater. If a connection/response is not received in that time, the next OCSP Responder/Repeater will be tried. The default is 10 seconds.

   Timeout: ______ (seconds)

4. Certificate used by the OCSP Responder/Repeater to sign its response. This is used to validate that the response from the OCSP Responder/Repeater is from a trusted source.

   Certificate: Please have file ready at install time.

3.2.2.1.2 User Lookup

In order to read other attributes that correspond to the authenticated user from Active Directory, the device will need to construct an LDAP query based on information obtained from the user's card.

1. The useful information on the card is described in *User Configuration Information* on page 2. Check the box next to the card information to use:

   ☐ User Principal Name – *12345678@mil*

   ☐ RFC822 Name – *joe.smith@branch.us.mil*

   ☐ Subject Name – *CN=SMITH.JOE.12345678, OU=Contractor, OU=PKI, OU=DoD, O=U.S. Government, C=US*

   ☐ EDIPI – *12345678*

2. The LDAP attribute representing the data read from the card as described in item 2 above is also required. For example, if User Principal Name is used, the LDAP attribute is usually "userPrincipalName".

LDAP Attribute: ____

3.2.2.2 Manual Login Configuration

If manual login is allowed, a button appears in the lower right corner of the login screen that says "Login". The user will press the Login button and be prompted for their username and password.

1. The default domain to be associated with usernames. In a Kerberos login, the id is typically: <domain>\<id> OR <id>@domain. By specifying the default domain, users will not need to provide the "domain\" or " @domain" part when entering their username. This value is typically the same as the Kerberos Realm (but in lowercase).

   Default Manual Login Domain: ____

2. In order to lookup information about the user, the LDAP Attribute that corresponds to the user's id is needed. This attribute is typically named: samaccountname.

   Manual Login Search Attribute: ____

3. If the username or password can contain non-US English characters, the code page used to process those characters must be set. The code page already configured on the device can be used or an explicit one can be used. Select the choice below:

   ☐ Device Default

   ☐ ISO 8859-2

   ☐ ISO 8859-5

   ☐ ISO 8859-9

   ☐ PC 858

3.3 User Authorization

In addition to providing user authentication, the PKI Authentication application can also provide user authorization to allow or disallow to the device as a whole or to individual functions on the device. The authorization is based on Active Directory groups; users can be allowed or denied access based on their membership to the specified groups.

1. User authorization can be enabled or disabled for the device. If you want to use User Authorization for the whole device or for individual device functions, this must be enabled. Do you want to enable this feature?

   ☐ Yes ☐ No

2. If User Authorization is enabled, the application must use an LDAP query to determine the Active Directory groups to which the user belongs. To use the MFP's default LDAP directory (this is the typical answer), check the Default Configuration option. To define a separate LDAP Configuration to use for this lookup, check one of the Custom Configuration options and complete the appropriate section.

   Check the box below to indicate the LDAP directory setup that will be used:

   ☐ LDAP – Default Configuration (as specified in section 2.5)

   ☐ LDAP – Configuration 1 (as specified in section 8.1)

   ☐ LDAP – Configuration 2 (as specified in section 8.2)

   ☐ LDAP – Configuration 3 (as specified in section 8.3)

3. If User Authorization is enabled, it can be used to restrict access to the device as a whole or just to individual functions. For device access, select the appropriate authorization setting.

   ☐ All Users Can Use the Device – no restrictions

   ☐ Only Users in the Groups specified in item 4 can use the device

   ☐ All Users Except those in the Groups specified in item 4 can use the device

4. If User Authorization is enabled and the device access setting in item 3 requires groups to be included or excluded, list the Active Directory group names here.

   ____

   ____

   ____

3.4 Logout Behavior

3.4.1 Auto-Logout

After a user has successfully authenticated to the device, there is an Auto-Logout timeout feature. If the user does not touch the screen within the specified time even with the SmartCard inserted in the reader, the PKI Authentication application will automatically logout and return to the enter pin screen (if using a SmartCard) or the login screen (if using manual login). This prevents another person from using the device in the event someone walks away without removing their SmartCard or logging out.

Auto-Logout Timeout in Seconds: ______ (3 to 900 seconds)

3.4.2 Card Removal

After a user has successfully authenticated to the device and the SmartCard is removed, it returns to the locked-out state. However, if a job is in progress when the card is removed, there are three options for what should happen.

Cancel Job and Return to Login Screen	When the card is removed, the current job is cancelled and the MFP returns to the locked-out state.
Complete Job and Return to Login Screen	When the card is removed, the current job is completed and then the MFP returns to the locked-out state.
Complete Job and Return to Options Screen	When a copy is being made and the card is removed, the current job is completed and the MFP returns to the copy screen. When the Home or Back button is pressed on the copy screen, the MFP returns to the locked-out state. For all other functions, the current job is completed and the MFP returns to the locked-out state.

Check which operation method desired when the card is removed while a job is in progress:

☐ Cancel Job and Return to Login Screen

☐ Complete Job and Return to Login Screen

☐ Complete Job and Return to Options Screen

4 PKI/AD Standard Applications Configuration

This application is used if User Authorization is needed for the standard copy, fax, and/or ftp device functions; otherwise, this application does not need to be installed. To use this application, the PKI/AD Authentication application must be installed and the User Authorization setting in that application must be enabled and configured. (See section 3.3 for more information.) To disable any of the standard device functions for all users, see the MFP Configuration Guide.

4.1 Copy

Copy access can be left open for all authenticated users or it can be restricted to certain Active Directory groups. If restricted to certain groups, Copy should not be enabled on the Login Screen. (See section 3.1.1 for more information).

1. If User Authorization is enabled, it can be used to restrict access to the Copy function. For copy access, select the appropriate authorization setting.

   □ All Users Can Make Copies – no restrictions

   □ Only Users in the Groups specified in item 2 can use make copies

   □ All Users Except those in the Groups specified in item 2 can make copies

2. If User Authorization is enabled and the device access setting in item 1 requires groups to be included or excluded, list the Active Directory group names here.

   ____

   ____

   ____

4.2 Fax

Fax access can be left open for all authenticated users or it can be restricted to certain Active Directory groups. If restricted to certain groups, Fax should not be enabled on the Login Screen. (See section 3.1.2 for more information).

1. If User Authorization is enabled, it can be used to restrict access to the Fax function. For fax access, select the appropriate authorization setting.

   ☐ All Users Can Send Faxes – no restrictions

   ☐ Only Users in the Groups specified in item 2 can use send faxes

   ☐ All Users Except those in the Groups specified in item 2 can send faxes

2. If User Authorization is enabled and the device access setting in item 1 requires groups to be included or excluded, list the Active Directory group names here.

   ____

   ____

   ____

4.3 FTP

FTP access can be left open for all authenticated users or it can be restricted to certain Active Directory groups.

1. If User Authorization is enabled, it can be used to restrict access to the FTP function. For FTP access, select the appropriate authorization setting.

   ☐ All Users Can Use FTP – no restrictions

   ☐ Only Users in the Groups specified in item 2 can use FTP

   ☐ All Users Except those in the Groups specified in item 2 can use FTP

2. If User Authorization is enabled and the device access setting in item 1 requires groups to be included or excluded, list the Active Directory group names here.

   ____

   ____

   ____

5 PKI/AD Email Configuration

This application is used to enhance the standard email functionality available on the device. The enhanced features available include:

- User Authorization to restrict access to certain Active Directory Groups
- Greater control of the Email User Interface
- Setting the From address to that of the authenticated user
- Limiting to whom emails can be sent
- Signing and Encrypting the email body and attachments

If email is disabled on the device or any of the enhanced features are not necessary, this application does not need to be installed.

5.1 Email User Authorization

Email access can be left open for all authenticated users or it can be restricted to certain Active Directory groups.

1. If User Authorization is enabled, it can be used to restrict access to the Email function. For email access, select the appropriate authorization setting.

   □ All Users Can Send Emails – no restrictions

   □ Only Users in the Groups specified in item 2 can send emails

   □ All Users Except those in the Groups specified in item 2 can send emails

2. If User Authorization is enabled and the device access setting in item 1 requires groups to be included or excluded, list the Active Directory group names here.

   ____

   ____

   ____

5.2 Email Server Setup

The Email Server Settings are usually configured as part of the initial MFP setup. If that has not been done, the following information will be needed.

1. IP Address or Hostname of SMTP Server and the port used (typically 25). A primary and secondary address can be specified.

   IP Address or Name: ____________________________ Port: _______

IP Address or Name: ___________________________________ Port: _______

2. SMTP servers may require some type of authentication before allowing an email to be sent. Select the authentication required by the SMTP Server.

   □ Anonymous

   □ User's Credentials

   □ Service Account
   Distinguished Name:____

   Password:______________ To be provided at installation _____

   If using "User's Credentials", the SMTP server address listed in item 1 needs to be the hostname and not the IP Address.

3. All emails sent from the device will have a default subject that can be changed (if allowed) by the user. A suggested default is: "Scanned Document".

   Default Email Subject: ____

4. All emails sent from the device will have a default message that can be changed (if allowed) by the user. A suggested default is: "Please see the attached document."

   Default Email Message: ____

   ____

   ____

5.3 User Options

There are several settings available that allow the user interface to be configured as to what options are available to the end user.

1. A default subject is configured on the device for all emails sent from the device. The user can also be given the option to change it. Is the user allowed to change the subject?

   □ Yes □ No

2. A default message is configured on the device for all emails sent from the device. The user can also be given the option to change it. Is the user allowed to change the message?

   □ Yes □ No

3. Default scan options (such as format, paper size, duplex, etc) are configured on the device for all emails sent from the device. The user can also be given the option to change the options. Is the user allowed to change the scan options?

   ☐ Yes ☐ No

4. By default, after an email is sent the user is returned to the Welcome Screen. The application can be configured so that the user is instead returned to the email screen with all the same options (send to, subject, message, and scan options) retained. This allows a user to quickly send multiple documents to the same destination(s). Should the multiple email option be enabled?

   ☐ Yes ☐ No

5.4 From Address

The PKI Email application provides the ability to set the *From* address to that of the authenticated user on the device. There are two possible sources for the email address:

Card Email Address	The SmartCard contains an RFC822 email ID (see *User Configuration Information* on page 2). This address is used as the user's email address.
LDAP Lookup	The email address of the user can be queried from one of the specified LDAP Configurations.

Check the box below to indicate the desired email address method. If Manual Login is allowed, LDAP Lookup should be used for all email addresses, since not all users will login with a SmartCard.

☐ Card Email Address ☐ LDAP Lookup

5.4.1 Card Email Address

The use of the Card Email address does not require any additional configuration information.

5.4.2 LDAP Lookup

The use of an LDAP lookup requires the LDAP configuration and lookup attributes to be specified. This is used to find the authenticated user's email address instead of using the one available on the card itself.

1. The LDAP directory to be used for the lookup needs to be specified. To use the LDAP directory defined for address book lookups (this is the typical answer), check the Default Configuration option. To define a separate LDAP Configuration to use for this lookup, check one of the Custom Configuration options and complete the appropriate section.

   Check the box below to indicate the LDAP directory setup that will be used:

□ LDAP – Default Configuration (as specified in section 2.5)

□ LDAP – Configuration 1 (as specified in section 8.1)

□ LDAP – Configuration 2 (as specified in section 8.2)

□ LDAP – Configuration 3 (as specified in section 8.3)

2. Regardless of the LDAP configuration used, the LDAP attribute representing the email address is needed. This attribute is typically named “mail”.

   Email Attribute: ____

5.5 To Address

The PKI Email Application has several options that can be used to configure the addresses to which an email can be sent.

1. The application can be configured to allow the user to only send email to his/herself or to others as well. When only sending to his/herself, the user’s email address is displayed but the user is given no option to add or otherwise modify the destinations. Select to whom the user can send email:

   □ User can only send email to self

   □ User can send email to self and/or others

2. The application can be configured to allow the user to send email to only certain domains. List the domains (if any) below that email destinations should be limited to. No wildcards can used; list the full domain for each domain that should be allowed.

   ____

   ____

   ____

3. The application can be configured to automatically set the *To* address to be the same as the *From* address. This allows a user to quickly send an email to him/herself. The user can easily clear his/her address or add another to the list. Do you want the *To* address automatically populated with the user’s email address?

   □ Yes □ No

4. The application can be configured to allow the user to search the global address list or book (also known as the GAL). Specify which LDAP Configuration should be used for this capability.

   □ LDAP – Default Configuration (as specified in section 2.5)

   □ LDAP – Configuration 1 (as specified in section 8.1)

   □ LDAP – Configuration 2 (as specified in section 8.2)

   □ LDAP – Configuration 3 (as specified in section 8.3)

5.6 Email Signing and Encryption

The application can be configured to digitally sign and/or encrypt the email message and attachments.

5.6.1 Email Signing

This feature is only available when a user is authenticated with a SmartCard. The certificate used to sign the email is taken from the signing certificate available on the card.

1. This feature can be always disabled, always enabled, or the user can be prompted. The prompt that appears depends on the encryption setting.

   □ Always Disabled

   □ Always Sign

   □ Prompt User

2. When the email is only signed (not encrypted), it can be signed so that the receiver of the email can read it even if his/her email client does not support digitally signed emails. Or it can signed so that only email clients that support digitally signed emails can view it. Which method should be used?

   □ Clear (All email clients can view the email)

   □ Opaque (Only email clients that support digital signatures can view the email)

3. Some specifications (such as the DOD CAC) require that the Non-Repudiation bit of the signing certificate be set in order for that certificate to be considered valid for digitally signing emails. Is the Non-Repudiation bit required?

   □ Yes □ No

5.6.2 Email Encryption

Emails can only be encrypted when the encryption certificate can be found for **each** of the recipients – this limits encrypted emails to those users in the global address book. The encryption certificate on the card (if available) is used for the authenticated user if he/she sends email to his/herself.

1. This feature can be always disabled, always enabled, or the user can be prompted. The prompt that appears depends on the signing setting.

   ☐ Always Disabled

   ☐ Always Sign

   ☐ Prompt User

2. When the email is both signed and encrypted, it can be signed once or twice. When signed twice, the email is signed, encrypted, and then the resulting message is signed again. Choosing the double-signing methods reduces the maximum allowed email size to approximately 15MB. Which method should be used?

   ☐ Sign and Encrypt

   ☐ Sign and Encrypt and Sign Again

3. The LDAP configuration designated for the Address Book Lookup in section 5.5 is used for searching for the encryption certificates. A primary and alternate LDAP attribute can be specified for the location of the user's certificates. The defaults are "userSMIMECertificate" and "userCertificate", respectively. If different attributes should be used, specify below.

   Primary LDAP Attribute: ____

   Alterrnate LDAP Attribute: ____

   The primary attribute is searched first; if no valid encryption certificate is found, the alternate attribute is searched. If no valid certificate is found, an error message is displayed and the email is cancelled.

5.6.3 Results

The following table details the results based on the email signing and encryptions specified above.

Email Signing	Email Encryption	Result
Disabled	Disabled	Email is sent without signing or encryption.
Always Sign	Disabled	Email is sent with digital signature but no encryption.
Prompt User	Disabled	User is prompted with: Do Not Sign the Email Sign the Email Email is sent not encrypted; signing is based on user's response.
Disabled	Always Encrypt	Email is always encrypted but not signed.
Disabled	Prompt User	User is prompted with: Do Not Encrypt the Email Encrypt the Email Email is sent not signed; encryption is based on user's response.
Always Sign	Prompt User	User is prompted with: Sign the Email Sign and Encrypt the Email Email is sent signed; encryption is based on user's response.
Prompt User	Always Encrypt	User is prompted with: Encrypt the Email Sign and Encrypt the Email Email is sent encrypted; signing is based on user's response.
Prompt User	Prompt User	User is prompted with: Do Not Sign or Encrypt the Email * Sign the Email Encrypt the Email Sign and Encrypt the Email Email signing and encryption is based on user's response.
Always Sign	Always Encrypt	Email is always sent signed and encrypted.

* If both settings are set to "Prompt User", the user can be required to sign or encrypt the email. In this case, the starred prompt is not displayed. Is the user required to sign and/or encrypt every email?

☐ Yes ☐ No

6 PKI/AD Scan to Network Configuration

The PKI Scan To Network application provides the ability to scan pages and store the resulting image onto a network fileshare. This application cannot be used in *Pin Only* mode.

6.1 General Settings

1. An icon is displayed on the device's Welcome screen. The icon allows the user to select the *Scan to Network* function. The text that appears above the Welcome screen icon can be customized. The default value is *Scan to Network.*

   Text: ____

2. If User Authorization is enabled, it can be used to restrict access to the Scan To Network function. This setting controls access to any fileshare; more restrictive access can be given to individual fileshares. For general Scan To Network access, select the appropriate authorization setting.

   □ All Users Can Send Emails– no restrictions

   □ Only Users in the Groups specified in item 3 can scan to network

   □ All Users Except those in the Groups specified in item 3 can scan to network

3. If User Authorization is enabled and the device access setting in item 1 requires groups to be included or excluded, list the Active Directory group names here.

   ____

   ____

   ____

6.2 Fileshare Settings

An unlimited of fileshares can be defined. Each fileshare can be a static pre-defined share or it can be dynamically created (such as the user's home directory) by getting information from LDAP. Each fileshare has the following settings.

1. Fileshare Authorization. Each fileshare can have its own user authorization. This is only available if User Authorization is enabled in PKI/AD Authentication application. If the user is not authorized, this fileshare is not displayed for the user to select. Select the user authorization for this fileshare.

   ☐ All Users Can Use This Fileshare – no restrictions

   ☐ Only Users in the Groups specified in item 2 can use this fileshare

   ☐ All Users Except those in the Groups specified in item 2 can use this fileshare

2. If User Authorization is enabled and the file shareaccess setting in item 1 requires groups to be included or excluded, list the Active Directory group names here.

   ____

   ____

3. Display Name. If the user has access to more than one fileshare, all the possible choices are displayed in a list. What name should be given to the fileshare?

   File Share Display Name: ______________________________

4. UNC Path. Each fileshare needs the UNC Path that corresponds to it. If looking up data from LDAP to create the UNC Path, use a "%u" (no quotes) in the path to represent the data. The "%u" will be replaced after the LDAP lookup by the actual data to create the actual UNC path.

   UNC Path: ______________________________

5. Replacement Value. If a "%u" was specified in the UNC Path (item 4), the value that replaces the "%u" must be selected. The value replacing "%u" is:

   ☐ User Principal Name

   ☐ Email Address

   ☐ EDI-PI

   ☐ LDAP Lookup using LDAP Configuration:

      ☐ LDAP – Default Configuration (as specified in section 2.5)

      ☐ LDAP – Configuration 1 (as specified in section 8.1)

      ☐ LDAP – Configuration 2 (as specified in section 8.2)

      ☐ LDAP – Configuration 3 (as specified in section 8.3

      LDAP Attribute: ______________________________

6. Default Filename. The default filename for the scanned file can be specified. The default value is *scanned-image.*

   Default Filename: ____

7. Rename File. The default filename can optionally be renamed by the user at scan time. The default value is to allow the user to rename the file.

   ☐ Yes, allow the file to be renamed ☐ No, the user cannot rename the file.

8. Append Timestamp. A timestamp can be appended to the filename. If the user is not allowed to change the default filename (see item 7 above), the timestamp will always be appended to the filename. The default value is to append the timestamp to the file.

   ☐ Yes, append the timestamp. ☐ No, do not append the timestamp.

9. Remove "$". For some fileshares, a dollar sign ("$") may be included in a subfolder name but must be removed in order to write to the fileshare. Should the dollar sign be removed?

   ☐ Yes ☐ No

10. Create Directory. If the directory specified does not exist, the scan to fileshare will fail. The application can be configured so that it creates the directory if does not exist. Should the directory be automatically created?

    ☐ Yes ☐ No

6.3 Fileshare Examples

All the settings in section 6.2 should be repeated for each fileshare that is needed. Below are some examples for several different ways of defining the UNC Path.

1. User's Home Directory

Display Name:	H: Drive
UNC Path:	%u
Replacement Value:	LDAP Lookup
Replacement Lookup:	LDAP – MFP Default + User's Credentials
Replacement Attribute:	homeDirectory

2. Department Fileshare

Display Name:	Dept A Files
UNC Path:	\\fileserver\deptshares\depta
Replacement Value:	Not Used
Replacement Lookup:	Not Used
Replacement Attribute:	Not Used

3. Fileshare based on User’s Windows ID

Display Name:	S: Drive
UNC Path:	\\fileserver\%u$
Replacement Value:	LDAP Lookup
Replacement Lookup:	LDAP – MFP Default + User’s Credentials
Replacement Attribute:	samaccountname

7 Finding Configuration Information

The sections describe various methods for obtaining some of the configuration information needed in the previous section.

7.1 Kerberos Realm

The quickest method to determine the Kerberos Realm is to use the Windows Resource Toolkit "klist" program from a Windows workstation with PKI logon. If the toolkit has not been installed on the workstation, it can be downloaded from the Microsoft Website by searching for "rktools.exe". Once the resource toolkit is installed, run

```
klist tgt
```

from a Windows command prompt. If the program is not found, change to the "C:\Program Files\Windows Resource Kits\Tools" directory to execute the program.

The program should list information similar to the following:

```
Cached TGT:

ServiceName: krbtgt
TargetName: krbtgt
FullServiceName: steve
DomainName: SMARTCARD.BP.LEXMARK.COM
TargetDomainName: SMARTCARD.BP.LEXMARK.COM
AltTargetDomainName: SMARTCARD.BP.LEXMARK.COM
TicketFlags: 0x40e00000
KeyExpirationTime: 0/38/4 0:00:10776
StartTime: 1/31/2007 8:41:47
EndTime: 1/31/2007 18:41:47
RenewUntil: 2/7/2007 8:41:47
TimeSkew: 2/7/2007 8:41:47
```

The Kerberos Realm is listed as the "DomainName". This value can be used as part of the information needed in section Active Directory, 3.2.2, item 2.

7.2 Domain Controller

The local administrator should know the domain controller(s) used for PKI authentication. If not, one of the following two methods can be used.

As part of the Windows Resource Toolkit, a program "nltest.exe" is installed. Run this program from the command line as follows:

```
nltest /dclist:<DOMAIN>
```

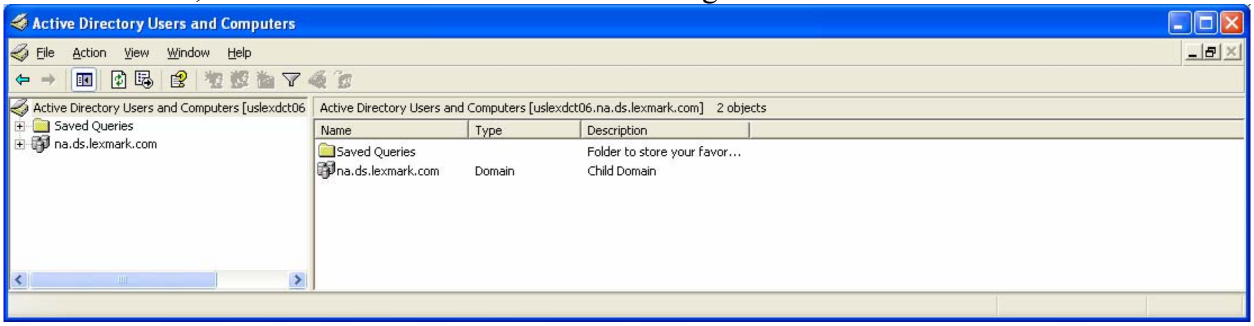
replacing `<DOMAIN>` with your actual domain. This will list the domain controllers for the specified domain. One of the servers will be listed with a `[PDC]` following its name. This is the primary domain controller; use that value as the first domain controller listed in section 3.2.2, item 1.

If that program is not available, you can try the following

1. Select Start | Run.

2. Type “dsa.msc”. This will launch the Active Directory Users and Computers Management Console. If a file not found error is received, go to Microsoft’s Website and search for “adminpak.msi”. Download and install the Windows 2003 Administration Tools Pack. Then start over at step 1.

3. Once launched, the domain is listed in the list on the right.



Active Directory Users and Computers [uslexdct06
Saved Queries
na.ds.lexmark.com

Active Directory Users and Computers [uslexdct06.na.ds.lexmark.com]   2 objects

Name	Type	Description
Saved Queries		Folder to store your favor...
na.ds.lexmark.com	Domain	Child Domain

4. Double-click the domain and then find the item called “Domain Controllers” in the list. The list of domain controllers will then be listed on the right.

5. Select one from the list and use that value as the first domain controller listed in section 3.2.2, item 1.

7.3 Kerberos Configuration File

When User Validation Mode is set to Active Directory, Kerberos must be configured on the MFP. The PKI Authentication Application allows for configuring the basic Kerberos settings without downloading a file to the MFP. For most environments, the basic settings will suffice and this step can be skipped. However, if your Kerberos setup involves multiple realms or requires other advanced settings, a Kerberos Configuration file must be created and downloaded to the MFP.

The Kerberos configuration file is an industry standard formatted file. An example is below with the critical elements described. `The example is in this font` ***while a description is in this font.***

The Kerberos Realm described in section 3.2.2, item 2 should be used to replace the *#####_DOMAIN.NAME.MIL_#####* text in the example below.

The IP address or fully qualified domain name for the Windows Domain Controller described in section 3.2.2, item 1 should be used for the *kdc* and *default_domain* fields in the *[realms]* section of the example below.

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = #####_DOMAIN.NAME.MIL_#####
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 12h

 default_etypes = arcfour-hmac-md5 des-cbc-md5 des-cbc-crc
 default_etypes_des = arcfour-hmac-md5 des-cbc-md5 des-cbc-crc

 default_tgt_enctypes = arcfour-hmac-md5 DES-CBC-MD5 DES-CBC-CRC
 default_tgs_enctypes = arcfour-hmac-md5 DES-CBC-MD5 DES-CBC-CRC

[appdefaults]

[realms]
```

Each supported Kerberos Realm needs to be listed in this section; repeat all of the following for each realm.

```
#####_DOMAIN.NAME.MIL_##### = {
```

KDCs can be listed in either ip address or fully qualified domain name. More than one KDC can be listed. If the first KDC cannot be contacted, then the next KDC is contacted. This process repeats until all KDCs are contacted. Note that if multiple KDCs are used, certificate chains will need to be present in the MFP for all KDCs.

```
  kdc = tcp/#####_ip_address_or_name_of_domain_controller_#####
  default_domain = #####_same_as_kdc_#####

  pkinit_require_eku = false
  pkinit_require_krbtgt_otherName = false
```

Microsoft implemented to "draft" versions of the IETF Kerberos PKINIT specifications. This resulted in some slight differences between software supporting the final IETF specification and those supporting the Microsoft implementations. This configuration flag informs the firmware to use the Microsoft format for PKINIT protocol commands.

```
  pkinit_win2k = yes
  pkinit_win2k_require_binding = no
}

[domain_realm]
```

Define a mapping between domain names found in the user's certificate and the Kerberos realm. The lines with "." allow for matching with names before suffix – i.e. "dc1.mil" matches ".mil" but not "mil". It is acceptable to map multiple domain names to the same realm.

```
.mil = #####_DOMAIN.NAME.MIL_#####
```

```
    mil = #####_DOMAIN.NAME.MIL_#####
```

If this configuration file is needed, use the above template to create the file and have it ready at install time.

7.4 LDAP Directory Information

Possible LDAP directories to use can be supplied by the Window Administrator. The Administrator will also have to determine the access rights: Anonymous, User's Credentials, or Service Account. The administrator may also be able to specify if SSL is required to be used.

A useful tool for browsing the LDAP directory is found at http://www.ldapbrowser.com. The standard version, not the administrator version, browser can be used. Microsoft supplies an LDP.EXE LDAP browser in some of their toolkits and support tools. LDP may already be loaded on a workstation. LDP has a less friendly user interface than the one provided by ldapbrowser.com.

Once the LDAP browser is available, the LDAP directory can be examined for the different data needed by the PKI applications.

7.5 Domain Controller Certificates

The local administrator should know how to obtain the certificates for the domain controller; they can typically be downloaded from an internal website. If this is not available, the certificates can also be located in the Windows workstation's certificate cache which can be examined using Internet Explorer.

In Internet Explorer version 6 or 7, the cache can be accessed in IE by going to: Tools | Internet Options | Content | Certificates.

Select the Intermediate Certification Authorities tab or the Trusted Root Certification Authorities tab. Find the certificate in the list; highlight it, and the click Export. For the format, choose Base-64 encoded X.509. Repeat this for each certificate that is needed. When finished, combine all the single text files into one text file, such as:

```
-----BEGIN CERTIFICATE-----
MIIE1jCCA76gAwIBAgIQY6sV0KL3tIhBtlr4gHG85zANBgkqhkiG9w0BAQUFADBs
…
l3DTbPe0mnIbTq0iWqKEaVne1vvaDt52iSpEQyevwgUcHD16rFy+sOnCaQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIE1zCCA7+gAwIBAgIQZWAEBZ+h+L5AKmbyl9hgSzANBgkqhkiG9w0BAQUFADBn
…
l3DTbPe0mnIbTq0iWqKEaVne1vvaDt52iSpEQyevwgUcHD16rFy+sOnCaQ==
-----END CERTIFICATE-----
```

Save this file and have it ready at install time.

8 Custom LDAP Configurations

Up to three custom LDAP Configurations in addition to the default LDAP configuration provided for Address Book Lookups can be specified on the device. If the default LDAP configuration can be used for all lookups, this section can skipped. However, if a custom LDAP configuration was specified as being needed for the user's email address lookup or the user's home directory lookup, then complete the following LDAP configuration information.

Please refer to section 2.5, *Default LDAP Configuration*, if more information is needed on any of these settings.

8.1 LDAP Configuration 1

1. Use KDC used for User Authentication as LDAP Server: ☐ (If yes, skip item 2.)

2. LDAP Server IP Address/Name: ____

3. LDAP Server Port: _______ (Typically: 389 for non-SSL, 636 for SSL)

4. SSL is required: ☐ (If required, please have the SSL certificate available.)

5. LDAP Certificate Validation: (Only necessay is SSL is being used.)

   ☐ Never ☐ Allow

   ☐ Try ☐ Demand

6. Information from the card used for the lookup:

   ☐ User Principal Name – *12345678@mil*

   ☐ RFC822 Name – *joe.smith@branch.us.mil*

   ☐ Subject Name – *CN=SMITH.JOE.12345678, OU=Contractor, OU=PKI, OU=DoD, O=U.S. Government, C=US*

   ☐ EDIPI – *12345678*

7. LDAP attribute representing the data read from the card:

   ____

8. Search Base: (Typically something like “ou=installation,dc=branch,dc=mil”)

   ____

9. Access rights needed to access the LDAP directory:

   ☐ Anonymous

   ☐ User’s Credentials (Cannot be used in Pin Only mode)

   ☐ Service Account

   Distinguished Name:______________________________________

   Password: _________ To be provided at installation _________

8.2 LDAP Configuration 2

1. Use KDC used for User Authentication as LDAP Server: □ (If yes, skip item 2.)

2. LDAP Server IP Address/Name: ____

3. LDAP Server Port: _______ (Typically: 389 for non-SSL, 636 for SSL)

4. SSL is required: □ (If required, please have the SSL certificate available.)

5. LDAP Certificate Validation: (Only necessay is SSL is being used.)

   □ Never □ Allow

   □ Try □ Demand

6. Information from the card used for the lookup:

   □ User Principal Name – *12345678@mil*

   □ RFC822 Name – *joe.smith@branch.us.mil*

   □ Subject Name – *CN=SMITH.JOE.12345678, OU=Contractor, OU=PKI, OU=DoD, O=U.S. Government, C=US*

   □ EDIPI – *12345678*

7. LDAP attribute representing the data read from the card:

   ____

8. Search Base: (Typically something like “ou=installation,dc=branch,dc=mil”)

   ____

9. Access rights needed to access the LDAP directory:

   □ Anonymous

   □ User’s Credentials (Cannot be used in Pin Only mode)

   □ Service Account

   Distinguished Name:____

   Password: _________ To be provided at installation _________

8.3 LDAP Configuration 3

1. Use KDC used for User Authentication as LDAP Server: ☐ (If yes, skip item 2.)

2. LDAP Server IP Address/Name: ____

3. LDAP Server Port: _______ (Typically: 389 for non-SSL, 636 for SSL)

4. SSL is required: ☐ (If required, please have the SSL certificate available.)

5. LDAP Certificate Validation: (Only necessay is SSL is being used.)

   ☐ Never ☐ Allow

   ☐ Try ☐ Demand

6. Information from the card used for the lookup:

   ☐ User Principal Name – *12345678@mil*

   ☐ RFC822 Name – *joe.smith@branch.us.mil*

   ☐ Subject Name – *CN=SMITH.JOE.12345678, OU=Contractor, OU=PKI, OU=DoD, O=U.S. Government, C=US*

   ☐ EDIPI – *12345678*

7. LDAP attribute representing the data read from the card:

   ____

8. Search Base: (Typically something like “ou=installation,dc=branch,dc=mil”)

   ____

9. Access rights needed to access the LDAP directory:

   ☐ Anonymous

   ☐ User’s Credentials (Cannot be used in Pin Only mode)

   ☐ Service Account

   Distinguished Name:____

   Password: _________ To be provided at installation _________

740 West New Circle Road
Lexington, KY 40550

www.lexmark.com