HP SmartCard NIPRNet Solution for US Government using non-FutureSmart firmware version

Administrator's Guide

HP SmartCard NIPRNet Solution for US Government using non-FutureSmart firmware version

Administrator's Configuration Guide

Copyright and License

The information contained herein is subject to change without notice.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Part number: CC543B

Edition: 3, 2/2016

Trademark credits

Table of contents

1 Introduction

The HP SmartCard NIPRNet Solution for US Government is designed to optimize security in imaging and printing environments for various Department of Defense (DoD) agencies and military branches of the US government.

This guide is intended for administrators responsible for managing security in their network environment and provides instructions on how to configure settings on supported HP products with a non-FutureSmart firmware version using the HP SmartCard NIPRNet Solution for US Government.

2 Getting started with HP SmartCard NIPRNet Solution for US Government

Get started by installing the HP SmartCard NIPRNet Solution for US Government on supported printers and updating the printer firmware, if required. This chapter provides information on the following topics:

- Supported Products
- Hardware installation
- Obtain the tools for HP SmartCard NIPRNet Solution

Supported Products

For a list of HP printers compatible with the HP SmartCard NIPRNet Solution for US Government, see Supported products.(c04896573)

Hardware installation

To configure the HP SmartCard NIPRNet Solution, purchase the “HP SmartCard US Govt NIPRNet Solution: CC543B #201”.

For the HP Smartcard NIPRNet Solution installation instructions, go to the: Installation Guide.

Obtain the tools for HP SmartCard NIPRNet Solution

The HPRC File Transfer Service (https://ftp.usa.hp.com/hprc) provides the firmware files, the Authentication Agent files, and the configuration information required to configure HP Multifunction Printers (MFPs). This site is periodically updated to identify the most current files required to install and configure the HP SmartCard NIPRNet Solution for US Government .

NOTE: Make sure to install the latest firmware and Authentication Agent files.

Follow these steps to download the tools required for the HP SmartCard NIPRNet Solution:

1. Go to HPRC File Transfer Service.
2. Read the **HPRC Terms of Use & Service**, and then click **Accept**.
3. Type in your Account name and password, and then click **Login**.

   NOTE: Passwords must be changed annually to the next consecutive number.

4. Click the **LATEST_Firmware** directory, and then click the Oz_olderdevice_firmware directory.

5. Download the following files and then save them in one folder:

   - Latest firmware file for your printer model

     OR

     Go to HP Support, and then select **Software and Drivers**.

     For instructions to download or update the firmware, go to Update the firmware using a USB flash drive or the Embedded Web Server (EWS).

   - Auth_agent file (usgovt_auth_agent_cac_v2.11.pjl or newer)

   - remove_cac_agent file (remove_cacagent.pjl)

   - FW update vbscript (FW_Update_14.2_FTP.vbs or the latest FW_Update file)

   When using File Transfer Protocol (FTP), the firmware update wizards automate the process of rebooting the firmware, authagent, and removing the cac agent.

   NOTE: If you cannot use FTP to upload the files to the HP printer, use Port Number “9100” to upload the files.

   Select the **FW_Update_Port_9100** directory and save the following files in the same folder — the firmware file, auth agent, remove agent, hpnpf, and the fw update vbscript.

   You can also use HP Web Jet Admin to update the firmware and upload the auth agent .pjl file.

6. Click the **Tools** directory.

7. Select one of the following files, and then click **Run** or **Save** to view the configuration information.

   - KerbosInfoCert2.exe

     OR

   - KerbosInfoCert2.vbs

   NOTE: Make sure to print this page to verify the Kerberos Client settings information when configuring the device.

8. Select the "CertificateChainBuilder.exe" file to export certificates, if desired.

   If downloading the “CertificateChainBuilder” executable file, follow these steps on the **Certificate Chain builder** user interface:

   a. On the **Server** section, select one of the following options:

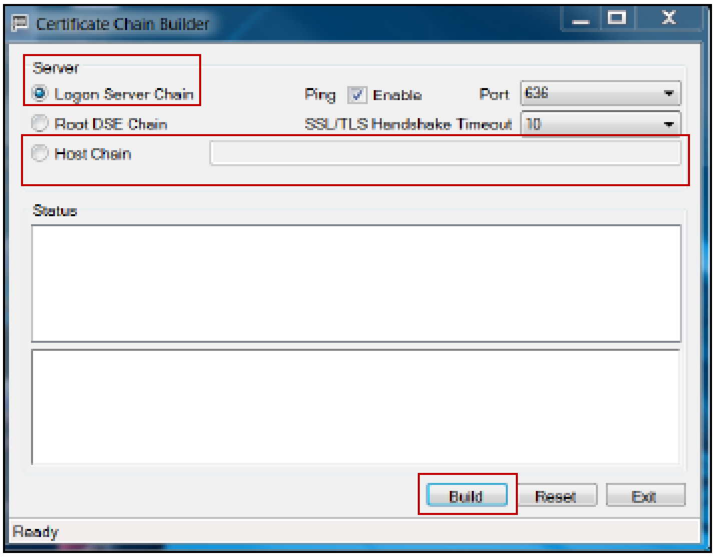
   - Logon Server Chain

   - Host Chain

     Type your full FQDN in the **Host Chain** text box.

b. Click **Build**.

Figure 2-1 Certificate Chain Builder



● Logon Server Chain

○ Root DSE Chain

○ Host Chain

Ping ☑ Enable

Port 636

SSL/TLS Handshake Timeout 10

3 Configure the printer using the Embedded Web Server (EWS)

Preview the following requirements of the HP Smartcard NIPRNET Solution for configuring the HP printer:

- HP Smartcard reader is properly installed
- Connected to Auth Agent version 2.11 or newer
- Upgraded to firmware version 14.2 or newer.

This chapter provides instructions on the below topics:

- Access the HP Embedded Web Server (EWS)
- Set the date and time on the HP device
- Verify the network settings
- Configure the HP product for Kerberos Authentication
- Configure validation of the certificates
- Configure authentication using the HP Smartcard reader
- Configure E-mail settings

Access the HP Embedded Web Server (EWS)

Follow these steps to open the EWS:

1. Open a Web browser, and in the address line, type the IP address of the printer exactly as it displays on the printer's control panel. Press the Enter key.

   NOTE: If the Web browser displays a message indicating that accessing the website might not be safe, select the option to continue to the website. Accessing this website will not harm the computer.

   NOTE: To prevent unauthorized changes in the printer configuration settings, IT administrators might set a password in the EWS.

2. Depending on how the HP EWS is configured, it might be necessary to log in using the administrator's password to access and configure printer settings.

   NOTE: If passwords are set in the EWS, only the **Information tab** will be available to the users.

Set the date and time on the HP device

NOTE: The device date and time must be synchronized to within five minutes of the date and time on the kerberos server. If the time difference is greater than five minutes, all HP Smartcard authentication attempts will fail.

1. Open the HP EWS.

   For instructions, see Access the HP Embedded Web Server (EWS) on page 5

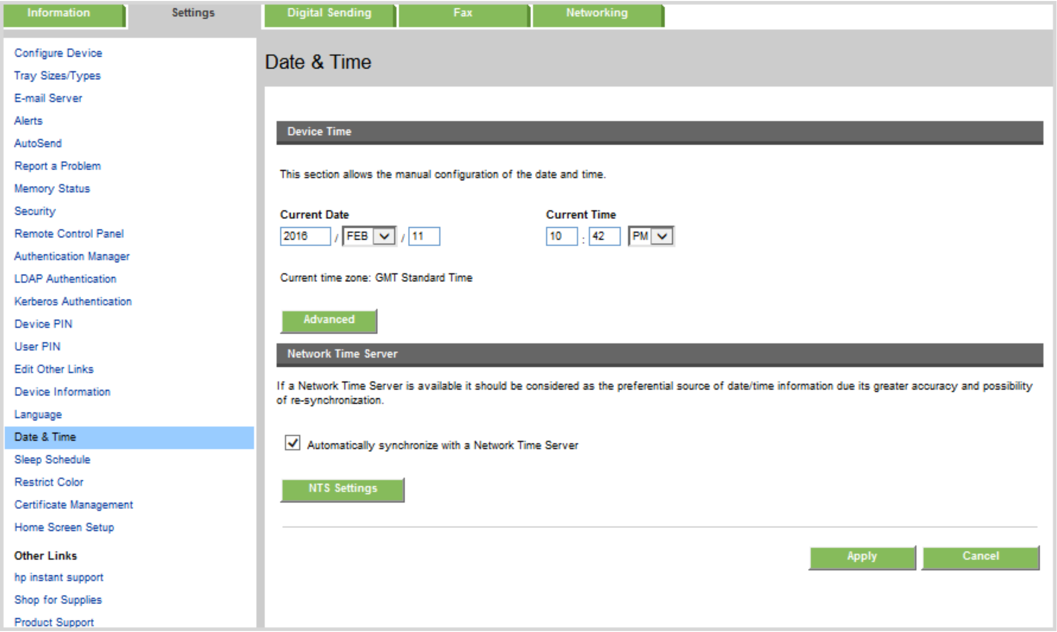
2. On the top navigation tabs, select the **Settings** tab.

3. In the left navigation pane, select **Date and Time**.

4. Type the **Current Date** and **Current Time**.

   To set the time zone or daylight savings time, click **Advanced**, select the **Time Zone** and **Daylight Savings Time**, and then click **OK**.

   Figure 3-1 Date & Time Settings



Date & Time

Device Time

This section allows the manual configuration of the date and time.

Current Date: 2016 / FEB / 11

Current Time: 10 : 42 PM

Current time zone: GMT Standard Time

Network Time Server

If a Network Time Server is available it should be considered as the preferential source of date/time information due its greater accuracy and possibility of re-synchronization.

☑ Automatically synchronize with a Network Time Server

5. Click **Apply** to save the changes.

Verify the network settings

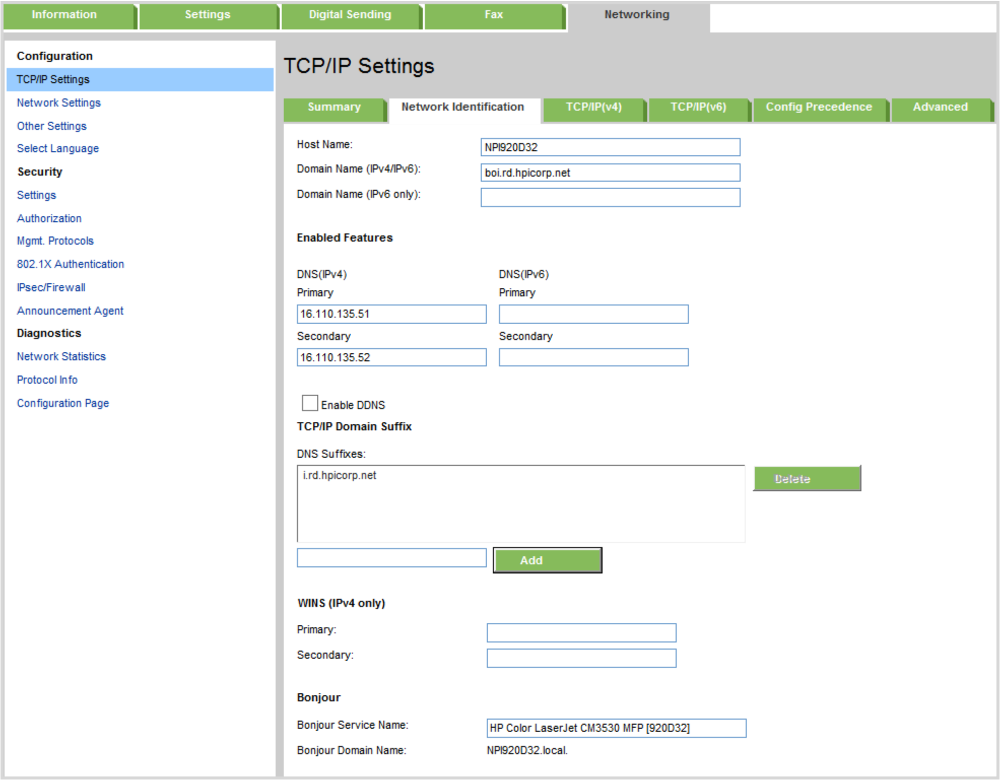
Use the following information to verify the HP device's TCP/IP network information.

1. Open a Web browser.

   For instructions, see Access the HP Embedded Web Server (EWS) on page 5

2. On the top navigation tabs, select the **Networking** tab.

3. In the left navigation pane, select **TCP/IP Settings**, and then select the **Network Identification** tab.



TCP/IP Settings

Host Name: NPI920D32

Domain Name (IPv4/IPv6): boi.rd.hpicorp.net

Domain Name (IPv6 only):

Enabled Features

DNS(IPv4)	DNS(IPv6)
Primary	Primary
16.110.135.51	
Secondary	Secondary
16.110.135.52	

☐ Enable DDNS

TCP/IP Domain Suffix

DNS Suffixes: i.rd.hpicorp.net

WINS (IPv4 only)

Primary:

Secondary:

Bonjour

Bonjour Service Name: HP Color LaserJet CM3530 MFP [920D32]

Bonjour Domain Name: NPI920D32.local.

4. Verify that the **Host Name** and **Domain Name (IPv4/IPv6)** are properly set.

5. Verify that the **DNS Primary** and **DNS Secondary** are correctly set.

6. If required, type additional DNS suffixes in the **DNS Suffixes** text box of the **TCP/IP Domain Suffix** section.

7. If applicable, type the WINS **Primary** and **Secondary** addresses in the **WINS (IPv4 only)** section.

8. Click **Apply** at the bottom of the page to save any changes.

Configure the HP product for Kerberos Authentication

NOTE: Make sure to configure and test the Kerberos settings when the HP Smartcard reader is installed for the first time.

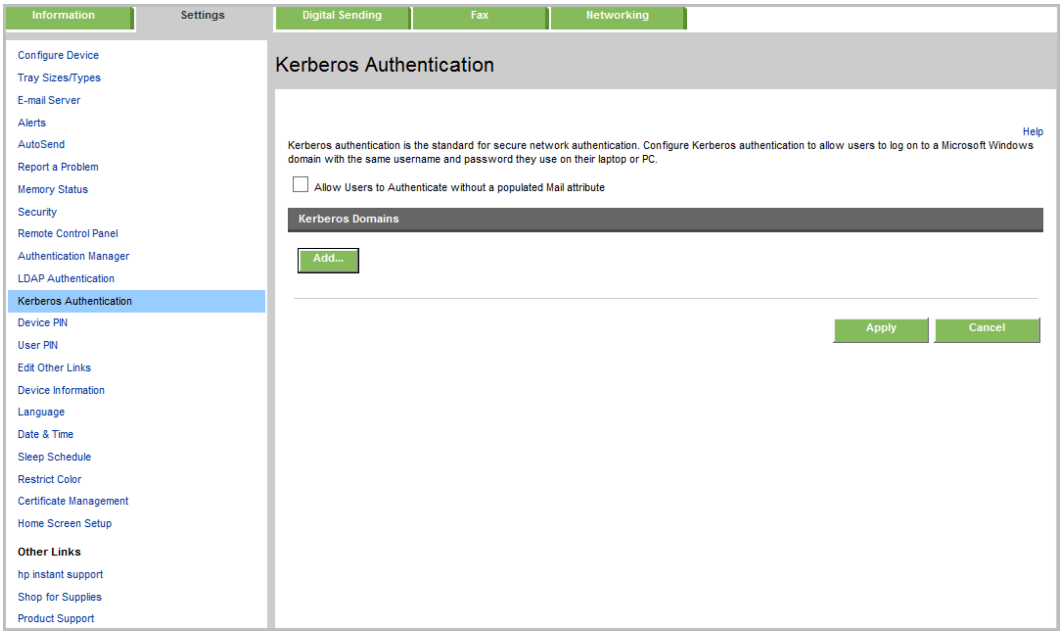
1. Open a Web browser.

   For instructions, see Access the HP Embedded Web Server (EWS) on page 5

2. On the top navigation tabs, select the **Settings** tab.

3. On the left navigation pane, select the **Kerberos Authentication** tab.

   Figure 3-2 Kerberos Authentication

   Kerberos Authentication

   Kerberos authentication is the standard for secure network authentication. Configure Kerberos authentication to allow users to log on to a Microsoft Windows domain with the same username and password they use on their laptop or PC.

   □ Allow Users to Authenticate without a populated Mail attribute

4. On the **Kerberos Authentication** page, click **Add**, and then complete the following steps to set parameters and credentials used to access the LDAP server:

   a. In the **Accessing the Kerberos Authentication Server** section, type the Kerberos domain name, OR click **Advanced** to access **Alternate Domain Configuration**.

   NOTE: Most US Government agencies disable the reverse DNS lookups option.

   - **Kerberos Realm:** Type the Kerberos domain in upper case.
   - **Kerberos Server Hostname:** Type the fully qualified domain name of the Kerberos realm.

     NOTE: The Kerberos Server Hostname might be the same as the Kerberos Realm if a Domain Name Service (DNS) is available and configured correctly. If a DNS is not available, use the IP address of the Kerberos Server.

   - **Kerberos Server Port:** The default port is 88.

NOTE: The default port might be different in different network environments. Contact your IT administrator to determine the appropriate port.

b. In the **Accessing the LDAP Server** section, complete the following information to access the LDAP server.

i. Select **Kerberos** or **Kerberos over SSL** from the **LDAP Server Bind Method** drop-down box.

ii. In the **Credentials** section, make sure that the **Use Device User's Credentials** option is selected.

iii. In the **LDAP Server** text box, type the server hostname.

The **LDAP Server** is usually the same as the Kerberos Server in the Windows Active Directory Environment.

iv. In the Port text box, type the port used by the LDAP protocol to communicate with the LDAP server.

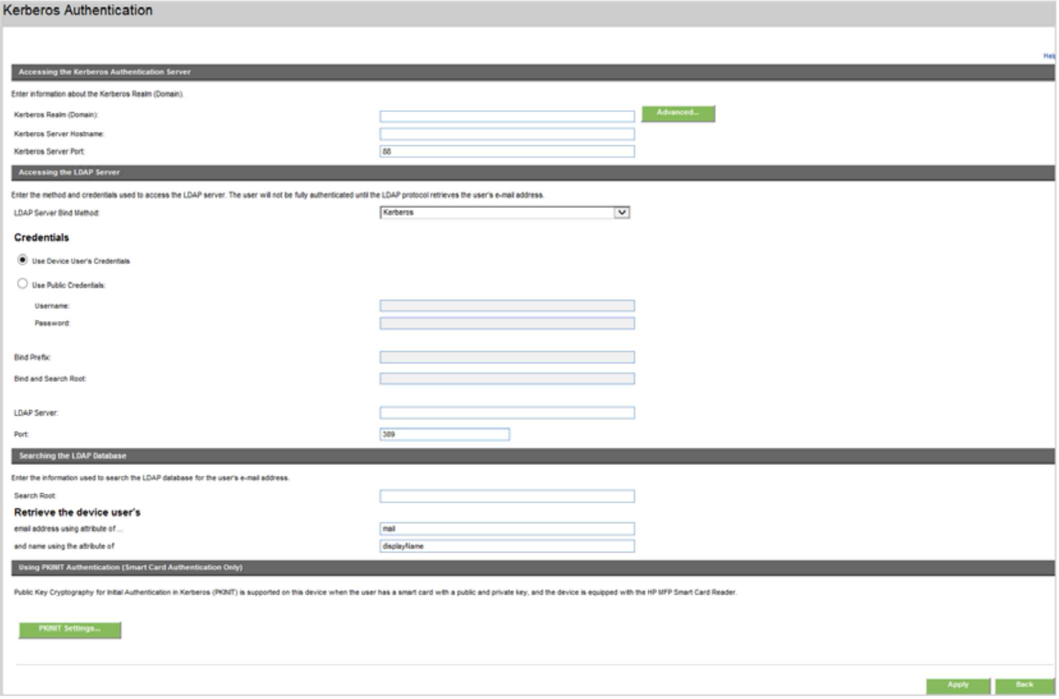
The port number is usually 389 or 636 or 3268 or 3269.

c. In the **Searching the LDAP Database** section, type the Search Root.

The Search Root is the distinguished name of the entry in the LDAP directory to search for addresses.

d. Click **PKINIT Settings**.

Figure 3-3 Kerberos Authentication setting



Kerberos Authentication

Accessing the Kerberos Authentication Server

Enter information about the Kerberos Realm (Domain).

Kerberos Realm (Domain):

Kerberos Server Hostname:

Kerberos Server Port: 88

Accessing the LDAP Server

Enter the method and credentials used to access the LDAP server. The user will not be fully authenticated until the LDAP protocol retrieves the user's e-mail address.

LDAP Server Bind Method: Kerberos

Credentials

● Use Device User's Credentials

○ Use Public Credentials:

Username:

Password:

Bind Prefix:

Bind and Search Root:

LDAP Server:

Port: 389

Searching the LDAP Database

Enter the information used to search the LDAP database for the user's e-mail address.

Search Root:

Retrieve the device user's

email address using attribute of ... mail

and name using the attribute of displayName

Using PKINIT Authentication (Smart Card Authentication Only)

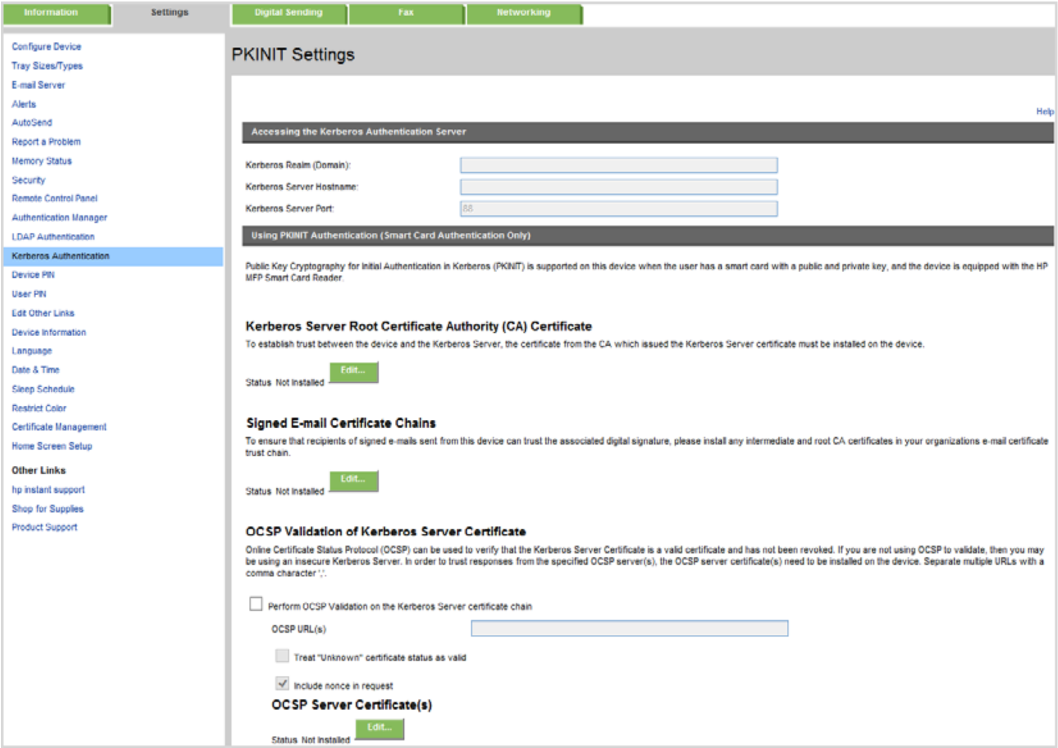
Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) is supported on this device when the user has a smart card with a public and private key, and the device is equipped with the HP MFP Smart Card Reader.

5. On the **PKINIT Settings** page, install the required certificates.

a. In the **Using PKINIT Authentication (Smart Card Authentication Only)** section, click **Edit**.

b. On the **Certificates** page, click **Browse**, locate the certificate, click **Import**, and then click **Back**. Click **Apply** on the **PKINIT Settings** page.

Figure 3-4 PKINIT Settings



PKINIT Settings

Accessing the Kerberos Authentication Server

Kerberos Realm (Domain):

Kerberos Server Hostname:

Kerberos Server Port: 88

Using PKINIT Authentication (Smart Card Authentication Only)

Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) is supported on this device when the user has a smart card with a public and private key, and the device is equipped with the HP MFP Smart Card Reader.

Kerberos Server Root Certificate Authority (CA) Certificate

To establish trust between the device and the Kerberos Server, the certificate from the CA which issued the Kerberos Server certificate must be installed on the device.

Status Not Installed

Signed E-mail Certificate Chains

To ensure that recipients of signed e-mails sent from this device can trust the associated digital signature, please install any intermediate and root CA certificates in your organizations e-mail certificate trust chain.

Status Not Installed

OCSP Validation of Kerberos Server Certificate

Online Certificate Status Protocol (OCSP) can be used to verify that the Kerberos Server Certificate is a valid certificate and has not been revoked. If you are not using OCSP to validate, then you may be using an insecure Kerberos Server. In order to trust responses from the specified OCSP server(s), the OCSP server certificate(s) need to be installed on the device. Separate multiple URLs with a comma character ','.

☐ Perform OCSP Validation on the Kerberos Server certificate chain

OCSP URL(s)

☐ Treat "Unknown" certificate status as valid

☑ Include nonce in request

OCSP Server Certificate(s)

Status Not Installed

Configure validation of the certificates

NOTE: Before configuring the certificate, make sure that your site uses Kerberos over SSL to install the Root CA Certificate.

Follow these steps to install certificates on the **Certificates** page of the HP Embedded Web Server (EWS).

1. Open a Web browser.

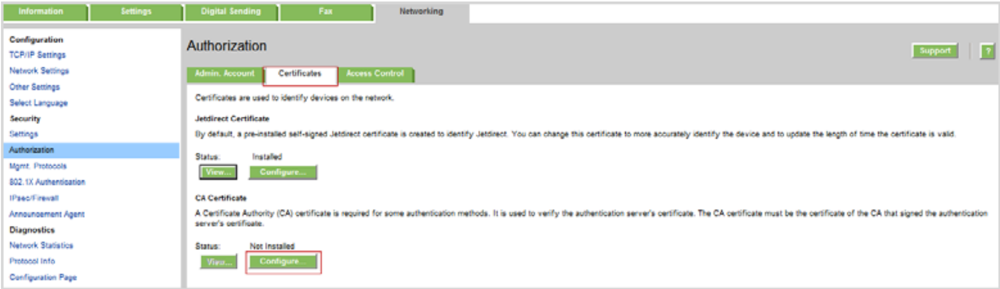
   For instructions, see Access the HP Embedded Web Server (EWS) on page 5.

2. On the top navigation tabs, select the **Networking** tab.

3. On the left navigation pane, select **Authorization**.

4. Select the **Certificates** tab, and then in the **CA Certificate** section click **Configure**.

   Figure 3-5 Authorization page in the EWS

   Certificates are used to identify devices on the network.

   Jetdirect Certificate

   By default, a pre-installed self-signed Jetdirect certificate is created to identify Jetdirect. You can change this certificate to more accurately identify the device and to update the length of time the certificate is valid.

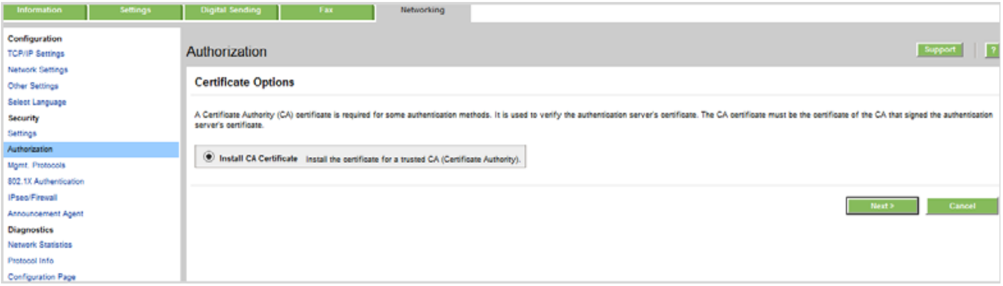
   Status: Installed

   CA Certificate

   A Certificate Authority (CA) certificate is required for some authentication methods. It is used to verify the authentication server's certificate. The CA certificate must be the certificate of the CA that signed the authentication server's certificate.

   Status: Not Installed

5. In the **Certificate Options** page, make sure that the **Install CA Certificate** option is enabled, and then click **Next**.

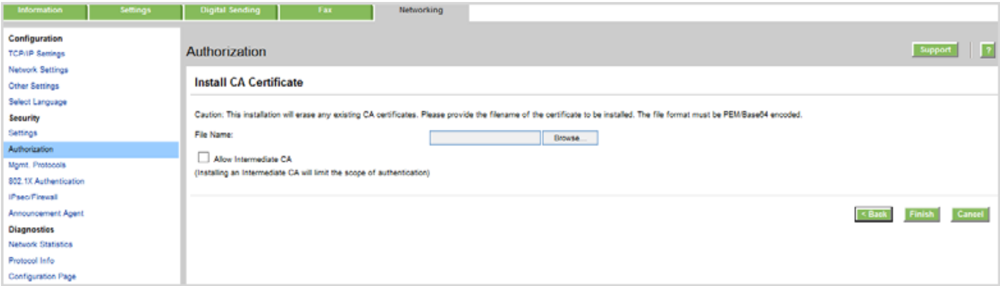
   Certificate Options

   A Certificate Authority (CA) certificate is required for some authentication methods. It is used to verify the authentication server's certificate. The CA certificate must be the certificate of the CA that signed the authentication server's certificate.

   ● Install CA Certificate Install the certificate for a trusted CA (Certificate Authority).

6. In the **Install CA certificates** page, complete the following steps to install the certificate:

   a. Click **Browse**



Authorization

Install CA Certificate

Caution: This installation will erase any existing CA certificates. Please provide the filename of the certificate to be installed. The file format must be PEM/Base64 encoded.

File Name:

□ Allow Intermediate CA

(Installing an Intermediate CA will limit the scope of authentication)

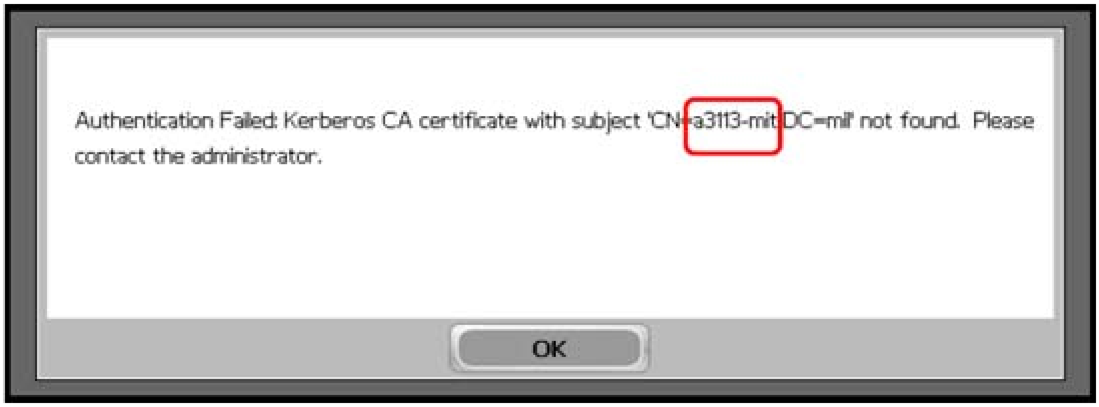
b. Select the Base-64 encoded certificate file, and then click **Finish**.

NOTE: This certificate is used for Kerberos Root CA

c. Make sure that the certificate is installed.

If the certificate is not correctly installed, an error message displays indicating the required missing certificate.

Figure 3-6 Authentication Failed



Authentication Failed: Kerberos CA certificate with subject 'CN=a3113-mit,DC=mil' not found. Please contact the administrator.

Configure authentication using the HP Smartcard reader

Follow these steps to configure the settings for the HP Smardcard reader:

1. Open a Web browser.

   For instructions, see Access the HP Embedded Web Server (EWS) on page 5

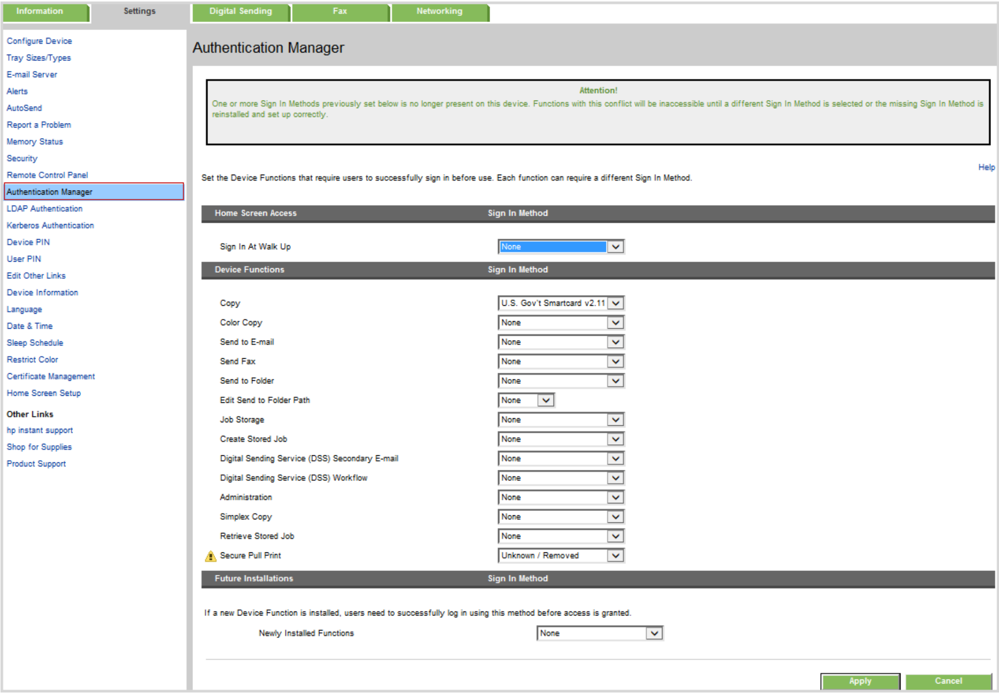
2. On the top navigation tabs, select the **Settings** tab.

3. On the left navigation pane, select **Authentication Manager**.

4. On the **Device Functions** section, select “US Govt Smartcard v2.11” or newer in the **Sign In Method** column.

5. Click **Apply**.

Figure 3-7 Authentication Manager



Authentication Manager

Attention!

One or more Sign In Methods previously set below is no longer present on this device. Functions with this conflict will be inaccessible until a different Sign In Method is selected or the missing Sign In Method is reinstalled and set up correctly.

Set the Device Functions that require users to successfully sign in before use. Each function can require a different Sign In Method.

Home Screen Access	Sign In Method
Sign In At Walk Up	None

Device Functions	Sign In Method
Copy	U.S. Gov't Smartcard v2.11
Color Copy	None
Send to E-mail	None
Send Fax	None
Send to Folder	None
Edit Send to Folder Path	None
Job Storage	None
Create Stored Job	None
Digital Sending Service (DSS) Secondary E-mail	None
Digital Sending Service (DSS) Workflow	None
Administration	None
Simplex Copy	None
Retrieve Stored Job	None
⚠ Secure Pull Print	Unknown / Removed

Future Installations	Sign In Method

If a new Device Function is installed, users need to successfully log in using this method before access is granted.

Newly Installed Functions: None

Configure E-mail settings

Use the **Digital Send** tab of the EWS to configure the address book, e-mail, and network folder settings.

- E-mail settings
- Address Book settings
- Configure Send to Folder settings

E-mail settings

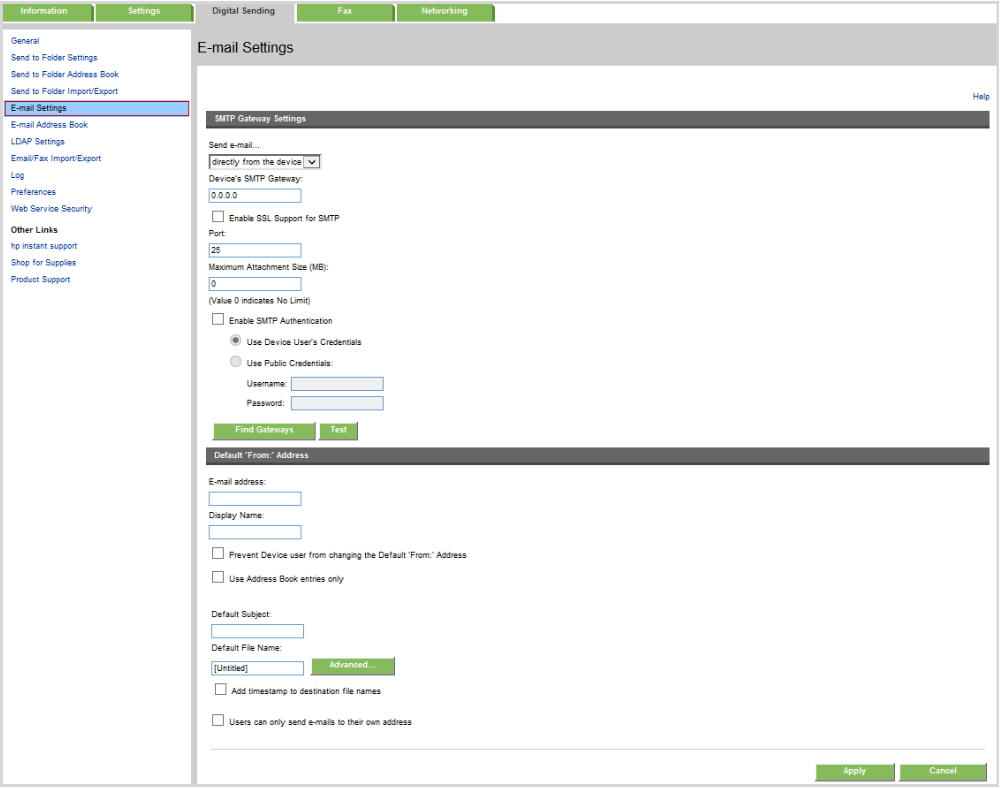
Use the following steps to configure the **E-mail Setup**.

1. Open a Web browser.

   For instructions, see Access the HP Embedded Web Server (EWS) on page 5.

2. On the top navigation tabs, select the **Digital Sending** tab.
3. On the left navigation pane, select **E-mail Settings**.
4. In the **SMTP Gateway Settings** section, type the SMTP gateway in the **Device's SMTP Gateway**.
5. In the **Default "From" Address**, make sure that an email address of the authenticated user displays in the **E-mail address** text box.
6. Click **Advanced**.

Figure 3-8 E-mail Settings: SMTP Gateway Settings



E-mail Settings

SMTP Gateway Settings

Send e-mail...

directly from the device

Device's SMTP Gateway:

0.0.0.0

□ Enable SSL Support for SMTP

Port:

25

Maximum Attachment Size (MB):

0

(Value 0 indicates No Limit)

□ Enable SMTP Authentication

● Use Device User's Credentials

○ Use Public Credentials:

Username:

Password:

Default 'From:' Address

E-mail address:

Display Name:

□ Prevent Device user from changing the Default 'From:' Address

□ Use Address Book entries only

Default Subject:

Default File Name:

[Untitled]

□ Add timestamp to destination file names

□ Users can only send e-mails to their own address

7. On the **Advanced E-mail Settings** page, follow these steps to configure the **S/MIME Settings (Signed/Encrypted E-mail)**:

   a. In the **Digital Signature** drop-down list, select **Sign Message**.

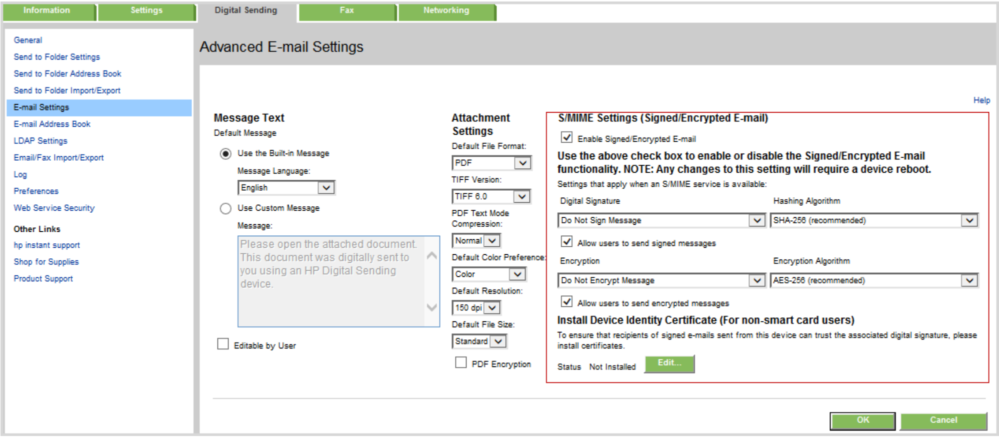
   b. In the **Hashing Algorthm** drop-down list, select **SHA-1**.

   c. In the **Encryption** drop-down list, make sure that the **Do Not Encrypt Message** is selected.

   d. In the **Encryption Algorithm** drop-down list, select the appropriate algorithm for your environment.

   e. Click **OK**.

Figure 3-9 Advanced E-mail Settings



Advanced E-mail Settings

Message Text

Default Message

● Use the Built-in Message

Message Language: English

○ Use Custom Message

Message: Please open the attached document. This document was digitally sent to you using an HP Digital Sending device.

□ Editable by User

Attachment Settings

Default File Format: PDF

TIFF Version: TIFF 6.0

PDF Text Mode Compression: Normal

Default Color Preference: Color

Default Resolution: 150 dpi

Default File Size: Standard

□ PDF Encryption

S/MIME Settings (Signed/Encrypted E-mail)

☑ Enable Signed/Encrypted E-mail

Use the above check box to enable or disable the Signed/Encrypted E-mail functionality. NOTE: Any changes to this setting will require a device reboot.

Settings that apply when an S/MIME service is available:

Digital Signature: Do Not Sign Message

Hashing Algorithm: SHA-256 (recommended)

☑ Allow users to send signed messages

Encryption: Do Not Encrypt Message

Encryption Algorithm: AES-256 (recommended)

☑ Allow users to send encrypted messages

Install Device Identity Certificate (For non-smart card users)

To ensure that recipients of signed e-mails sent from this device can trust the associated digital signature, please install certificates.

Status Not Installed

Address Book settings

Use the following steps to configure the **Address Book** settings.

1. Open a Web browser.

   For instructions, see Access the HP Embedded Web Server (EWS) on page 5

2. On the top navigation tabs, select the **Digital Sending** tab.

3. On the left navigation pane, select **LDAP Settings**.

4. Select the **Allow Device to directly access an LDAP Address Book** check box.

5. In the Accessing the LDAP Server, complete the following steps:

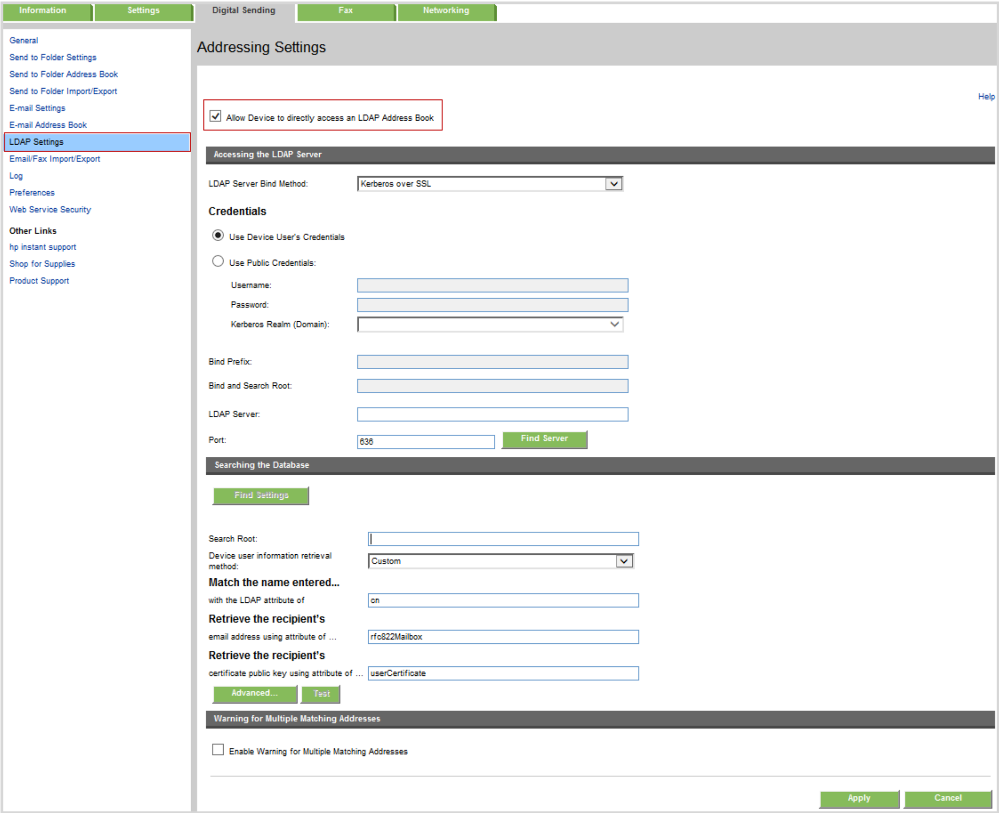
   a. In the **LDAP Server Bind Method** drop-down list, select **Kerberos over SSL**.

   b. In the **Credentials** section, make sure that the **Use Device's User's Credentials** is selected.

   c. In the **LDAP Server** text box, type the Kerberos server used in the Windows Active Directory Environment.

d. In the **Port** text box, type the Port number.

Figure 3-10 Address Settings: Accessing LDAP server



Addressing Settings

☑ Allow Device to directly access an LDAP Address Book

Accessing the LDAP Server

LDAP Server Bind Method: Kerberos over SSL

Credentials

● Use Device User's Credentials

○ Use Public Credentials:

Username:

Password:

Kerberos Realm (Domain):

Bind Prefix:

Bind and Search Root:

LDAP Server:

Port: 636

Searching the Database

Search Root:

Device user information retrieval method: Custom

Match the name entered...

with the LDAP attribute of cn

Retrieve the recipient's

email address using attribute of ... rfc822Mailbox

Retrieve the recipient's

certificate public key using attribute of ... userCertificate

Warning for Multiple Matching Addresses

□ Enable Warning for Multiple Matching Addresses

6. In the **Searching the Database** section, type the search root in the **Search Root** text box.

NOTE: If required, type specific attributes, or use the default attributes displayed on the page.

7. Click **Apply**.

Configure Send to Folder settings

Use the following steps to configure the **Send to Folder Settings**.

- Set up the Send to Folder settings
- Create a Home Directory
- Create Shared folders

Set up the Send to Folder settings

Use the following steps to set up **Send to Folder Settings** in the EWS.

1. Open a Web browser.

   For instructions, see Access the HP Embedded Web Server (EWS) on page 5

2. On the top navigation tabs, select the **Digital Sending** tab.

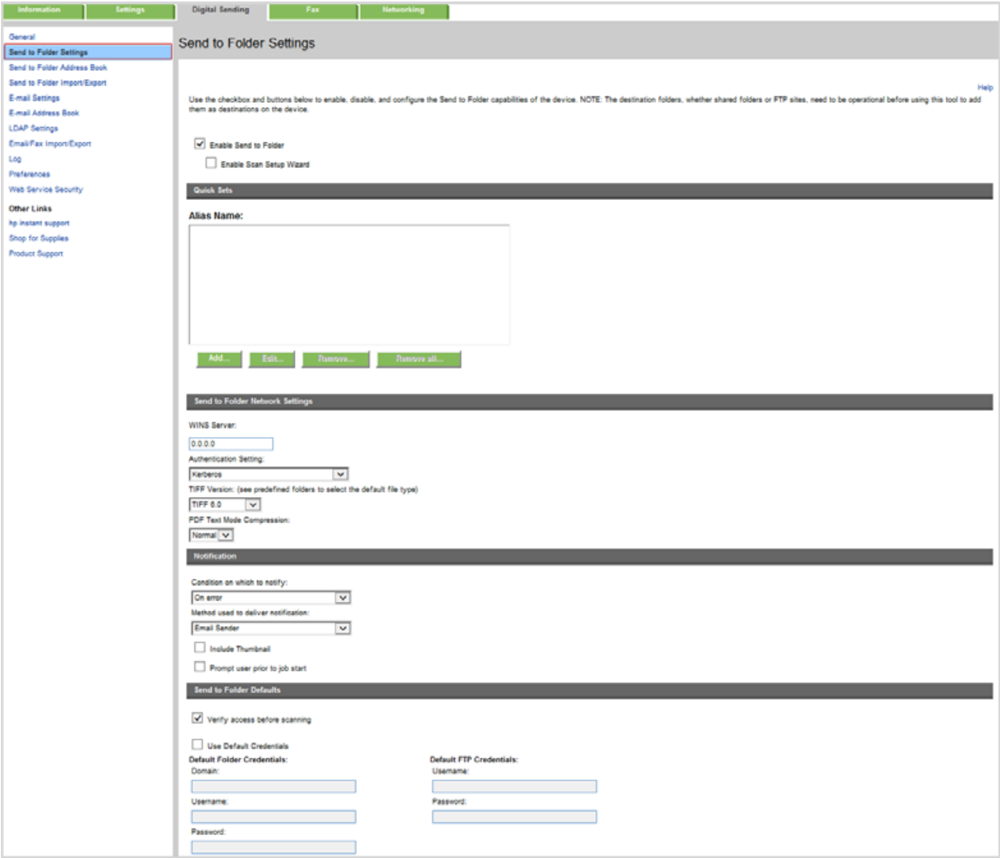
3. On the left navigation pane, select **Send to Folder Settings**.

4. Select the **Enable Send to Folder** check box.

5. In the **Send to Folder Network Settings** section complete the following steps:

   a. In the **Authentication Setting** drop-down list, select **Kerberos**.

   b. Click **Apply**.



Send to Folder Settings

Use the checkbox and buttons below to enable, disable, and configure the Send to Folder capabilities of the device. NOTE: The destination folders, whether shared folders or FTP sites, need to be operational before using this tool to add them as destinations on the device.

☑ Enable Send to Folder

□ Enable Scan Setup Wizard

Quick Sets

Alias Name:

Send to Folder Network Settings

WINS Server: 0.0.0.0

Authentication Setting: Kerberos

TIFF Version: (see predefined folders to select the default file type) TIFF 6.0

PDF Text Mode Compression: Normal

Notification

Condition on which to notify: On error

Method used to deliver notification: Email Sender

□ Include Thumbnail

□ Prompt user prior to job start

Send to Folder Defaults

☑ Verify access before scanning

□ Use Default Credentials

Default Folder Credentials:

Domain:

Username:

Password:

Default FTP Credentials:

Username:

Password:

Create a Home Directory

Follow these steps to create a Home Directory

1. Open a Web browser.

   For instructions, see Access the HP Embedded Web Server (EWS) on page 5

2. On the top navigation tabs, select the **Digital Sending** tab.

3. On the left navigation pane, select **Send to Folder Settings**.

4. Select the **Enable Send to Folder** check box.

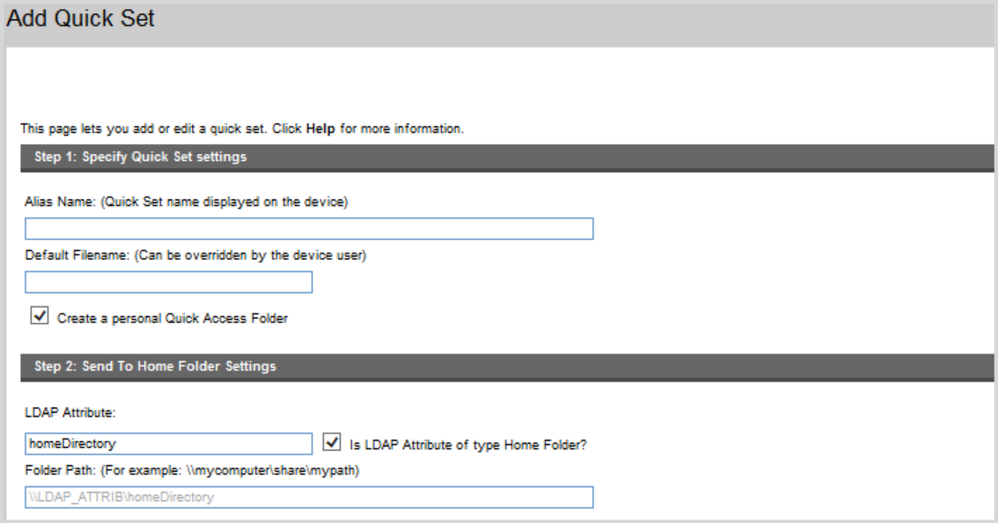
5. In the **Quick Sets** section, click **Add**.

6. On the **Add Quick Set** page, in **Step 1: Specify Quick Set settings**, select the **Create a personal Quick Access folder** check box.

NOTE: Step 2 will display the **Home Directory** attribute.

7. Click **OK**.

Figure 3-11 Add Quick Set



Add Quick Set

This page lets you add or edit a quick set. Click **Help** for more information.

Step 1: Specify Quick Set settings

Alias Name: (Quick Set name displayed on the device)

Default Filename: (Can be overridden by the device user)

☑ Create a personal Quick Access Folder

Step 2: Send To Home Folder Settings

LDAP Attribute: homeDirectory ☑ Is LDAP Attribute of type Home Folder?

Folder Path: (For example: \\mycomputer\share\mypath) \\LDAP_ATTRIB\homeDirectory

Create Shared folders

Follow these steps to create shared folders:

1. Open a Web browser.

   For instructions, see Access the HP Embedded Web Server (EWS) on page 5

2. On the top navigation tabs, select the **Digital Sending** tab.

3. On the left navigation pane, select **Send to Folder Settings**.

4. Select the following check boxes:

   - **Enable Send to Folder**
   - **Enable Scan setup Wizard**

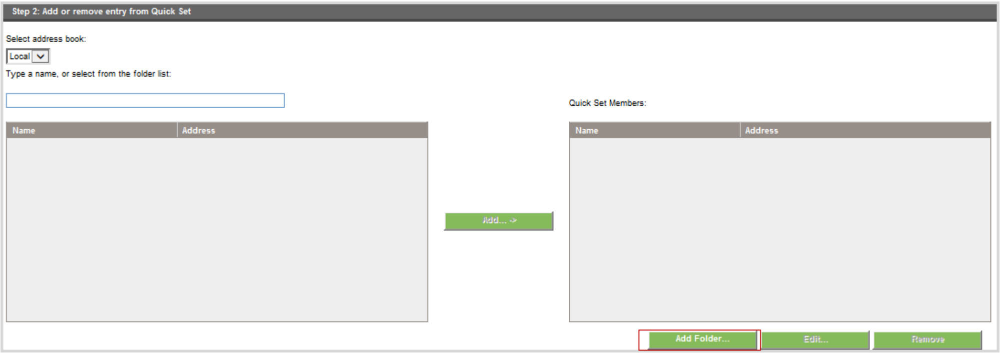
5. In the **Send to Folder Network Settings** section, select **Kerberos** from the **Authentication Setting** drop-down list.

6. In the **Quick Sets** section, click **Add**.

7. In the **Add Quick Set** page, complete the following steps:

   a. In **Step 1: Specify Quick Set settings**, type the alias name.

b. In **Step 2: Add or remove entry from Quick Set**, click **Add Folder**.



Select address book: Local

Step 2: Add or remove entry from Quick Set
Type a name, or select from the folder list:
Quick Set Members:
Name
Address
Name
Address
Add... ->
Add Folder...
Edit...
Remove

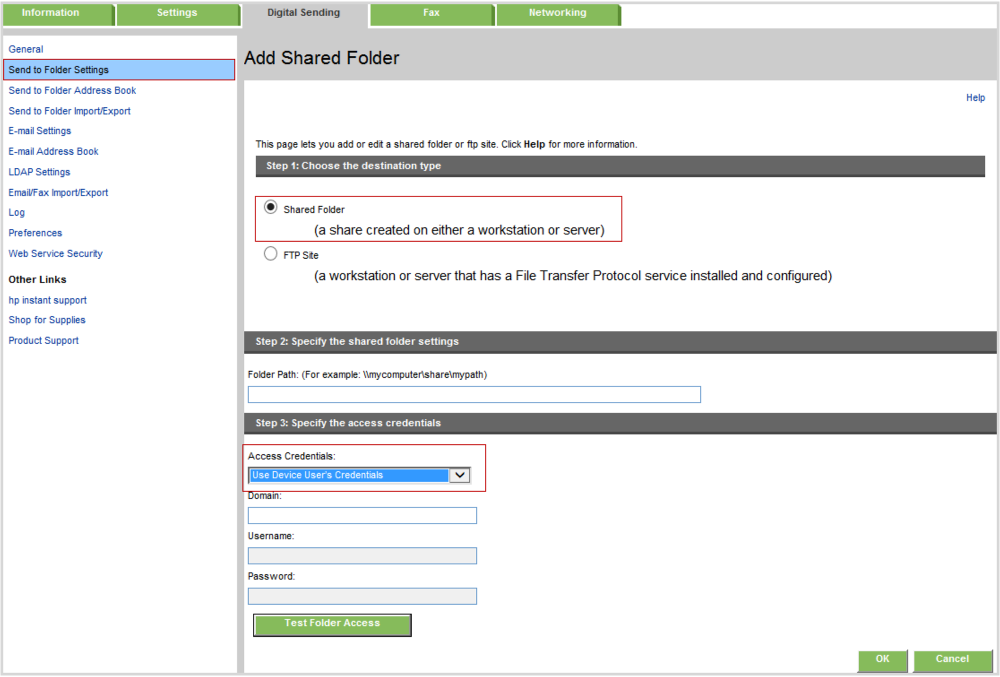
Figure 3-12 Add Folder

c. On the **Add Shared Folder** page, complete the following steps:

i. Select the **Shared Folder** option.

ii. In the **Step 3: Specify the access credentials** section, select **Use Device User's Credentials** from the **Access Credentials** drop-down list.

8. Click **OK**



Add Shared Folder

This page lets you add or edit a shared folder or ftp site. Click **Help** for more information.

Step 1: Choose the destination type

● Shared Folder
(a share created on either a workstation or server)

○ FTP Site
(a workstation or server that has a File Transfer Protocol service installed and configured)

Step 2: Specify the shared folder settings

Folder Path: (For example: \\mycomputer\share\mypath)

Step 3: Specify the access credentials

Access Credentials: Use Device User's Credentials

Figure 3-13 Shared Folder settings

A Licenses

This solution from HP uses and contains open source code and libraries from Heimdal Kerberos 5, OpenLDAP, OpenSC, and OpenSSL. Following are acknowledgements, copyrights, and license information associated with these open source solutions.

- Heimdal Kerberos
- OpenLDAP
- OpenSC
- OpenSSL
- SHA-2

Heimdal Kerberos

This product contains Heimdal Kerberos in binary form. Use of this software is governed by the terms of the license below:

Copyright © 1995 - 2009 Kungliga Tekniska Högskolan (Royal Institute of Technology, Stockholm, Sweden).

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the Institute nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenLDAP

This product contains OpenLDAP in binary form. Use of this software is governed by the terms of the license below:

The OpenLDAP Public License

Version 2.7, 7 September 2001

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright © 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

This product contains engine_pkcs11 in binary form. Use of this software is governed by the terms of the license below:

Copyright © 2002 Juha Yrjola. All rights reserved.

Copyright © 2001 Markus Friedl.

Copyright © 2003 Kevin Stefanik

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

OpenSC

OpenSC Credits

OpenSC was written by (or uses code copied from):

- Alon Bar-Lev
- Andrea Frigido
- Andreas Jellinghaus
- Antonino Iacono
- Antti Partanen
- Antti Tapaninen
- Benjamin Bender
- Bert Vermeulen
- Boris Kröger
- Bud P. Bruegger
- Carlos Prados
- Chaskiel Grundman
- Danny De Cock
- David Corcoran
- Douglas E. Engert
- Eric Dorland
- Franz Brandl
- Geoff Thorpe
- Gürer Özen for TUBITAK / UEKAE
- Jamie Honan
- Jean-Pierre Szikora
- João Poupino
- Joe Phillips
- Juan Antonio Martinez
- Juha Yrjölä
- Jörn Zukowski
- Kevin Stefanik
- Ludovic Rousseau

- Marc Bevand
- Marie Fischer
- Markus Friedl
- Martin Paljak
- Mathias Brossard
- Matthias Brüstle
- Nils Larsch
- Olaf Kirch
- Peter Koch
- Priit Randla
- Robert Bihlmeyer
- Sirio Capizzi
- Stef Hoeben
- Timo Teräs
- Todd C. Miller
- Viktor Tarasov
- Villy Skyttä
- Weitao Sun
- Werner Koch
- William Wanders

and

- Zetes
- g10 Code GmbH
- [http://www.opentrust.com/ OpenTrust] (ancient Idealx)
- Dominik Fischer

License

OpenSC does not include the official PKCS#11 header file, because that file is under a non-free license. Instead OpenSC contains a rewritten header file from scute project under this license:

/* pkcs11.h Copyright 2006, 2007 g10 Code GmbH Copyright 2006 Andreas Jellinghaus This file is free software; as a special exception the author gives unlimited permission to copy and/or distribute it, with or without modifications, as long as this notice is preserved. This file is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY, to the extent permitted by law; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. */

OpenSC (signer) also includes header file:

Java Runtime Interface Copyright (c) 1996 Netscape Communications Corporation. All rights reserved. dp Suresh <dp@netscape.com>

OpenSC also includes a copy of [http://www.geocities.com/bsittler/ my_getopt]:

my_getopt - a command-line argument parser Copyright 1997-2001, Benjamin Sittler

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

OpenSC can be compiled with OpenSSL:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

OpenSC uses autoconf m4 macros by

m4/autoconf macros by Bruno Haible

Copyright (C) 2001-2005 Free Software Foundation, Inc.

Copyright (C) 2002, 2003 Free Software Foundation, Inc.

using pkg-config and pkg.,4 autoconf macro by

Copyright (C) 2004 Scott James Remnant

OpenSC includes svn2cl by

svn2cl Arthur de Jong

Copyright (C) 2004, 2005 Arthur de Jong.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSC includes strlcpy.c (from ftp://ftp.openbsd.org/pub/OpenBSD/src/lib/libc/string/) by

Copyright (c) 1998 Todd C. Miller <Todd.Miller@courtesan.com>

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED “AS IS” AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

OpenSC can be compiled with zlib:

This product includes general purpose compression software written by Jean-loup Gailly and Mark Adler for the 'Zlib' project (http://www.zlib.net).

Copyright (C) 1995-2010 Jean-loup Gailly and Mark Adler

OpenSSL

This product contains OpenSSL in binary form. Use of this software is governed by the terms of the license below:

Copyright © 1998-2003 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

SHA-2

This product may include the following software in binary form: SHA-2 implementation by Olivier Gay. Use of this software is governed under terms of the following license:

FIPS 180-2 SHA-224/256/384/512 implementation

Last update: 02/02/2007

Issue date: 04/30/2005

Copyright (C) 2005, 2007 Olivier Gay (olivier.gay@a3.epfl.ch).

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

B Warranty Service

HP Limited Warranty Statement

HP Product	Duration of Limited Warranty
HP SmartCard NIPRNet Solution for US Government for U. S. Government	1 Year

1. HP warrants to you, the original end-user customer, that HP hardware and accessories will be free from defects in materials and workmanship after the original date of purchase, for the period specified above. If HP receives notice of such defects during the warranty period, HP will, at its option, either repair or replace, products, that prove to be defective. Replacement products may be either new or equivalent in performance to new. If the original end-user customer transfers the HP hardware and accessories to another user, warranty service is available to that user only for the remainder of the original warranty period. This Limited Warranty applies only to authentic HP-branded hardware products sold by or leased from Hewlett-Packard Company, its worldwide subsidiaries, affiliates, authorized resellers, or authorized country/region distributors.

2. HP warrants to you that HP software will not fail to execute its programming instructions after the date of purchase, for a period specified above, due to defects in material and workmanship when properly installed and used. If HP receives notice of such defects during the warranty period, HP will replace software that does not execute its programming instructions due to such defects.

3. HP does not warrant that the operation of HP products will be uninterrupted or error free. If HP is unable, within a reasonable time, to repair or replace any product to a condition as warranted, you will be entitled to a refund of the purchase price upon prompt return of the product.

4. HP products may contain remanufactured parts equivalent to new in performance or may have been subject to incidental use.

5. Warranty does not apply to defects resulting from (a) improper or inadequate maintenance or calibration, (b) software, interfacing, parts or supplies not supplied by HP, (c) unauthorized modification or misuse, (d) operation outside of the published environmental specifications for the product, or (e) improper site preparation or maintenance.

6. TO THE EXTENT ALLOWED BY LOCAL LAW, THE ABOVE WARRANTIES ARE EXCLUSIVE AND NO OTHER WARRANTY OR CONDITION, WHETHER WRITTEN OR ORAL, IS EXPRESSED OR IMPLIED AND HP SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, AND FITNESS FOR A PARTICULAR PURPOSE. Some countries/regions, states or provinces do not allow limitations on the duration of an implied warranty, so the above limitation or exclusion might not apply to you. This warranty gives you specific legal rights and you might also have other rights that vary from country/region to country/region, state to state, or province to province.

7. HP’s limited warranty is valid in any country/region or locality where HP has a support presence for this product and where HP has marketed this product. The level of warranty service you receive may vary according to local standards. HP will not alter form, fit or function of the product to make it operate in a country/region for which it was never intended to function for legal or regulatory reasons.

8. TO THE EXTENT ALLOWED BY LOCAL LAW, THE REMEDIES IN THIS WARRANTY STATEMENT ARE YOUR SOLE AND EXCLUSIVE REMEDIES. EXCEPT AS INDICATED ABOVE, IN NO EVENT WILL HP OR ITS SUPPLIERS BE LIABLE FOR LOSS OF DATA OR FOR DIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL (INCLUDING LOST PROFIT OR DATA), OR OTHER DAMAGE, WHETHER BASED IN CONTRACT, TORT, OR OTHERWISE. Some countries/regions, states or provinces do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

THE WARRANTY TERMS CONTAINED IN THIS STATEMENT, EXCEPT TO THE EXTENT LAWFULLY PERMITTED, DO NOT EXCLUDE, RESTRICT OR MODIFY AND ARE IN ADDITION TO THE MANDATORY STATUTORY RIGHTS APPLICABLE TO THE SALE OF THIS PRODUCT TO YOU.

Customer self-repair warranty service

HP products are designed with many Customer Self Repair (CSR) parts to minimize repair time and allow for greater flexibility in performing defective parts replacement. If during the diagnosis period, HP identifies that the repair can be accomplished by the use of a CSR part, HP will ship that part directly to you for replacement. There are two categories of CSR parts: 1) Parts for which customer self repair is mandatory. If you request HP to replace these parts, you will be charged for the travel and labor costs of this service. 2) Parts for which customer self repair is optional. These parts are also designed for Customer Self Repair. If, however, you require that HP replace them for you, this may be done at no additional charge under the type of warranty service designated for your product.

Based on availability and where geography permits, CSR parts will be shipped for next business day delivery. Same-day or four-hour delivery may be offered at an additional charge where geography permits. If assistance is required, you can call the HP Technical Support Center and a technician will help you over the phone. HP specifies in the materials shipped with a replacement CSR part whether a defective part must be returned to HP. In cases where it is required to return the defective part to HP, you must ship the defective part back to HP within a defined period of time, normally five (5) business days. The defective part must be returned with the associated documentation in the provided shipping material. Failure to return the defective part may result in HP billing you for the replacement. With a customer self repair, HP will pay all shipping and part return costs and determine the courier/carrier to be used.