



HP LaserJet Pro Devices – Installing 2048 bit SSL certificates

Table of Contents

Disclaimer	2
Introduction	2
Generating a Certificate Signing Request	2
The normal process	2
HP LaserJet Pro devices that support generating a 2048 bit certificate request	4
When the printer cannot generate a Certificate Request for 2048 bit certificates	5
Method 1 – Software supplied by the CA	5
Method 2 – OpenSSL	10
Obtaining a certificate from the CA	12
Installing the Certificate into the Printer	14
Converting the Certificate to the Personal Information Exchange (.PFX) format	15
Method 1 – Software supplied by the CA	15
Method 2 - OpenSSL	20
Installing the new certificate	21
Applicable Products	25
For more information	26
Call to action	26

Disclaimer

This document makes reference to certain products and/or services provided by third parties. These references are provided for example and demonstration purposes only and are not intended as an endorsement of any products, services, or companies.

Introduction

A recent publication of the National Institute of Standards and Technology (**NIST Special Publication 800-131A**) announced that the use of 1024 bit SSL/TLS certificates is no longer recommended and will be “disallowed” after December 31, 2013. The publication recommends the use of 2048 bit certificates to maintain network security and integrity. As a result, most Certificate Authorities (CAs) will no longer issue 1024 bit certificates. And, most Web browsers will no longer honor such certificates as safe and secure. In order to avoid error messages and the risk of a security breach, systems and devices that rely on the SSL/TLS protocols will need to have 2048 bit Certificates installed.

Most HP LaserJet printers can accept a 2048 bit certificate but some cannot generate the request needed to obtain one. This white paper will describe methods that can be used to obtain and install a 2048 bit certificate for such products. For more detailed information on the SSL/TLS protocols and the use of certificates to provide Internet safety and security, see “**HP Jetdirect and SSL/TLS**”.

There are three steps to this process:

1. Generate a Certificate Signing Request (CSR) for the printer
2. Obtain the certificate from a Certificate Authority (CA)
3. Import the certificate and private key into the printer

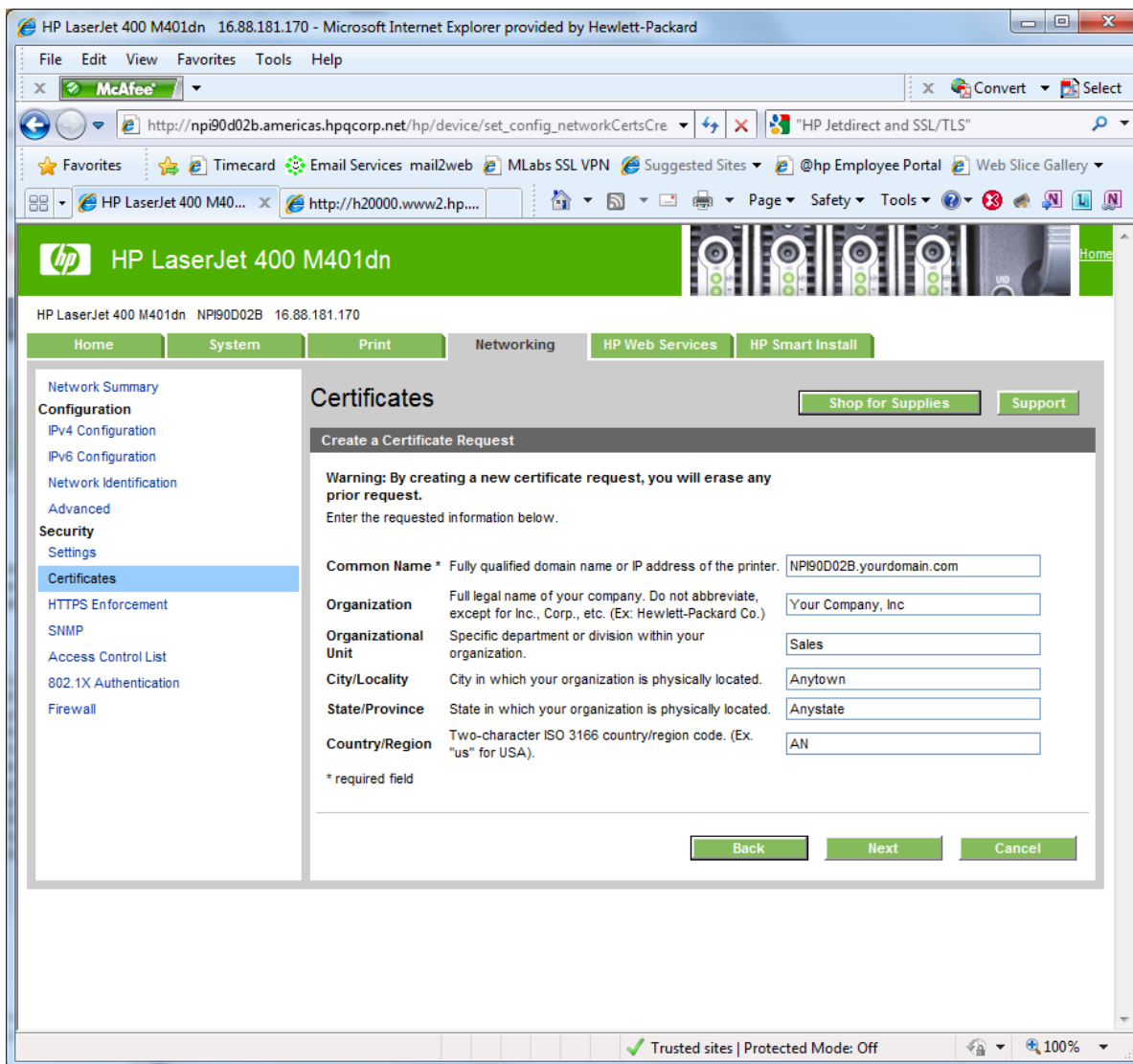
Generating a Certificate Signing Request

The normal process

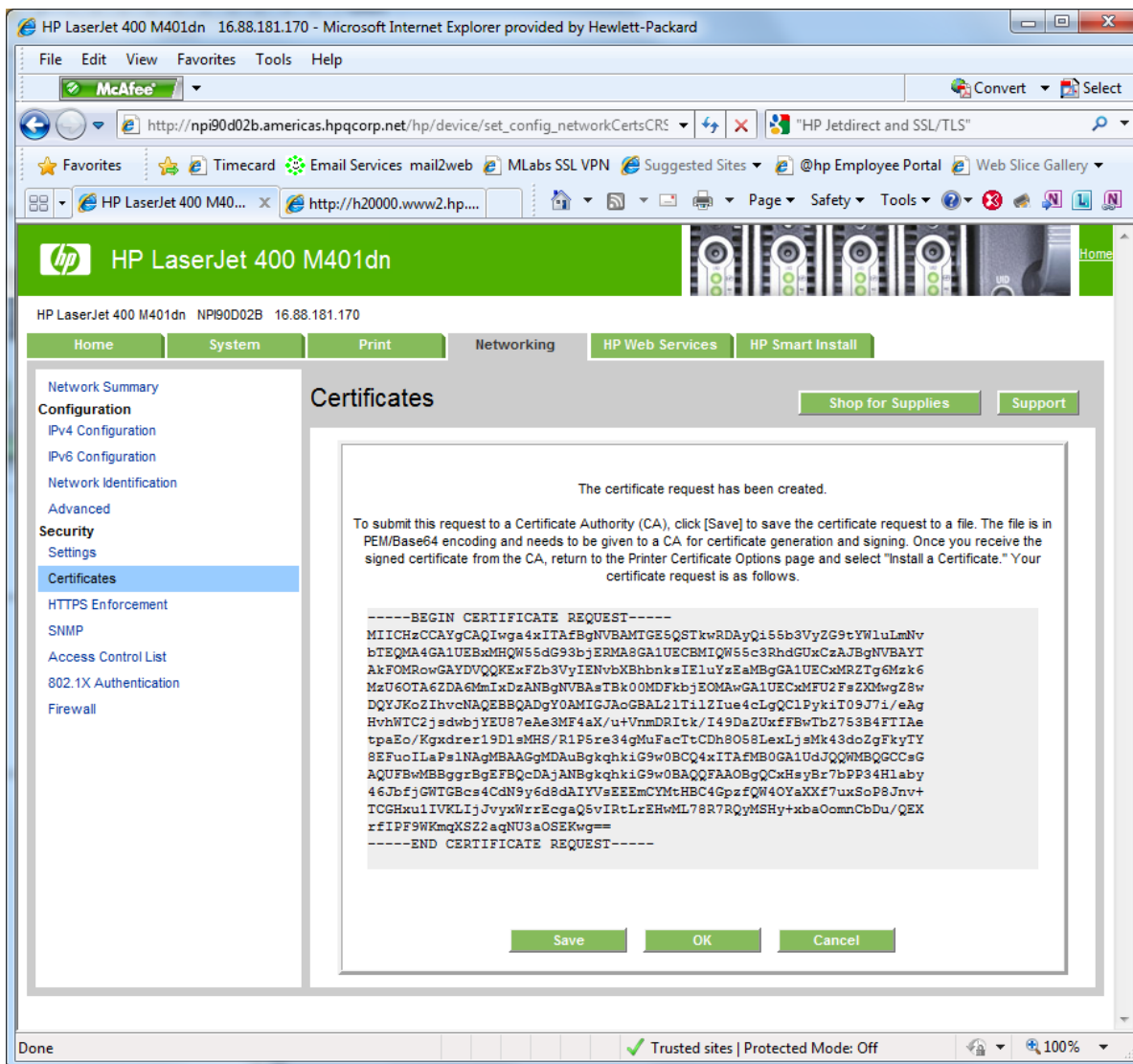
Ordinarily, a certificate is obtained from a Certificate Authority (CA) by submitting a “Certificate Signing Request” (CSR). This is a base 64 encoded text file which contains all the information needed by the CA to generate a certificate.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICyDCCAbACAQAwgYIxCzAJBgNVBAYTAkFOMREwDwYDVQQIEwhBbn1zdGF0ZTEQ
MA4GA1UEBxMHQW55dG93bjEOMAwGA1UECxMFU2FsZXNMGzAZBgNVBAoTE11vdXIg
Q29tcGFueSwgSW55jLjEhMB8GA1UEAxMYT1BJOTBEMDJCLn1vdXJkb21haW4uY29t
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAFVz7Ix1t4LgXdAR3znK
fx9f9bSBQooaIp4d7jK5kT67fix+0Pr5W0/XakYb4J2d+rTFnamu6B5XRXqqKXsA
z1DlpVZ/cVMTk2fhLTuzhxG0KDeouvTgRtq+AYcTeY0CNZ2nzOERxEvPU70zKHcD
krhjm2fvHvcCNWmiz9CCKVR3AtjMg90MJd9BoNMebyR8cf6IoAcgGaz5bth7zkf
myvFz3p+YGQfPxcMOzifZ1entV00nyirjBK5j1PuQ/wzZiacPEAKmbVJD+Xmt9+d
YxvVWtW3Z9JBpnHiH0YJwiFUzYyttRS+VL9FR5HDj+HrXaWMQ91X1BMSghDoIAK8
2wIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAFuWVxEokMfPr8kThMO0usD0bGcR
TRiK/mG5nkJqhhnVfd/8s1aCuMUcVBdw0fxWfQpyrHiIMP364DYozkeweaa1nGc
viZyNhWQsGym30G0H4OkNDXZQXi6X6GXvR0PwM/0aN7y94ki9mR2BOYmjNU9uPNZ
+xQ9kKERgsdmfZQpoEUq7rQ+gJiORU5rVzbn8XZtZ1xKzJUT3dReD16Yy9W7v66V
TcS+B7nhqnggNGfz5x7Fex0pyjtb3OJ2i5QMY4ODTYtIrURDEuK5/50qSTRVYweE
d/hZi9HyZlDrEFkBD0VsUSKFsGPsrbDAK4JEHYoL1FxsNW3drBiGMApuKmk=
-----END NEW CERTIFICATE REQUEST-----
```

Most devices that employ the SSL/TLS protocols provide a method to accept appropriate input from the user and generate a CSR. HP LaserJet printers are no exception. Those that support the SSL/TLS protocols include a page on their Embedded Web Server (EWS) devoted to generating CSRs.



When the data is entered and the "Next" button is pressed, the printer proceeds to generate the CSR (which contains encoded versions of the information above and a "public" key). A "private key" is also generated at this time and stored away in a safe place on the user's computer.



At this point the CRS can be saved as a file or copied directly into the online form provided by a CA. This is the best (and easiest) method to use if the printer can generate a CSR for a 2048 bit certificate. The next section will outline procedures to use when the printer can only generate a CSR for a 1024 bit certificate.

HP LaserJet Pro devices that support generating a 2048 bit certificate request

NOTE: If your device is listed below, skip the next section “When the printer cannot generate a Certificate Request for 2048 bit certificates” and go to “Installing the New Certificate” to install the certificate received from the Certificate Authority.

- HP LaserJet Pro 200 color Printer M251n (firmware date code 20140521 or later required)
- HP LaserJet Pro 200 color Printer M251nw (firmware date code 20140521 or later required)
- HP LaserJet Pro 200 color MFP M276n (firmware date code 20140521 or later required)
- HP LaserJet Pro 200 color MFP M276nw (firmware date code 20140521 or later required)
- HP LaserJet Pro M401a (firmware date code 20140521 or later required)
- HP LaserJet Pro M401d (firmware date code 20140521 or later required)
- HP LaserJet Pro M401dn (firmware date code 20140521 or later required)

- HP LaserJet Pro M401 dne (firmware date code 20140521 or later required)
- HP LaserJet Pro M401 dw (firmware date code 20140521 or later required)
- HP LaserJet Pro M401 n (firmware date code 20140521 or later required)
- HP LaserJet Pro M425dn (firmware date code 20140521 or later required)
- HP LaserJet Pro M425dw (firmware date code 20140521 or later required)
- HP LaserJet Pro M435nw MFP
- HP Color LaserJet Pro MFP M476dn
- HP Color LaserJet Pro MFP M476dw
- HP Color LaserJet Pro MFP M476nw
- HP LaserJet Pro 500 color MFP M570dn
- HP LaserJet Pro 500 color MFP M570dw
- HP LaserJet Pro M521 dn MFP
- HP LaserJet Pro M521 dw MFP
- HP LaserJet Pro M701a Printer
- HP LaserJet Pro M701n Printer
- HP LaserJet Pro M706n Printer

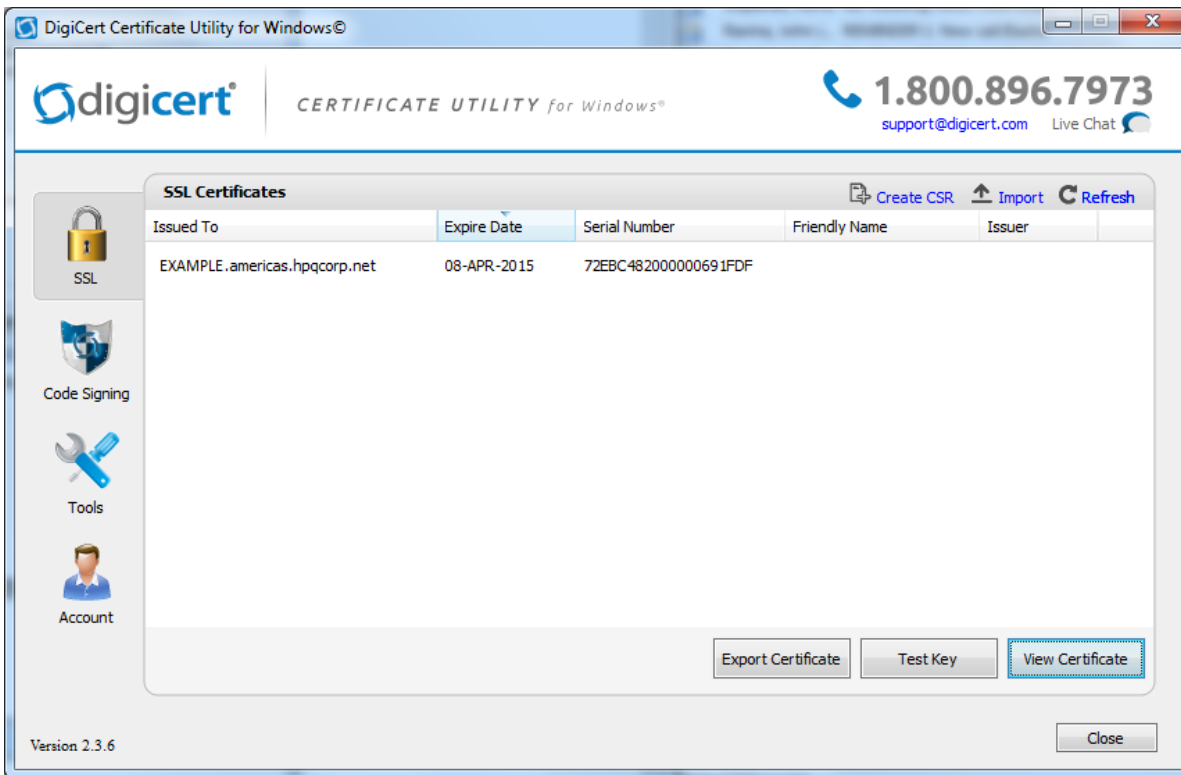
When the printer cannot generate a Certificate Request for 2048 bit certificates

Some HP LaserJet printers were designed before 2048 bit Certificates were declared the new standard. Many of these will have a firmware update that provides the ability to generate 2048 bit CSR. So, it's always a good idea to install the latest firmware (which can be obtained on HP.com) before resorting to the following procedures. However, some printers will never have this capability. The following procedures can be used for these.

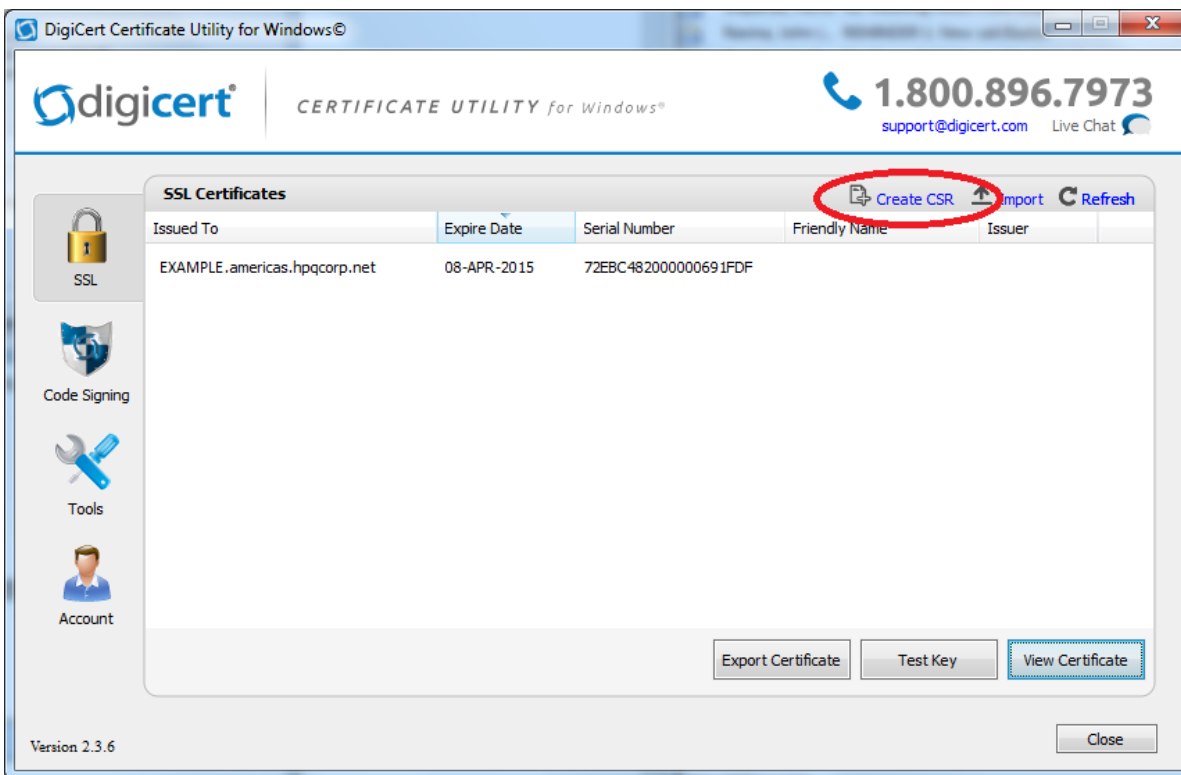
Warning: Do not be tempted to obtain a certificate from a CA that includes the private key along with it (either in separate files or combined in a .PFX or .P12 file). The private key is to be kept private. It is never to be shared with anyone else. Doing so will circumvent any security that the certificate is intended to provide.

Method 1 – Software supplied by the CA

Some CAs supply free software that can be used to generate a CSR outside the printer. Once the CSR is generated, it can be submitted to any CA (not just the one that provided the software). One such program is **DigiCert's Certificate Utility:**



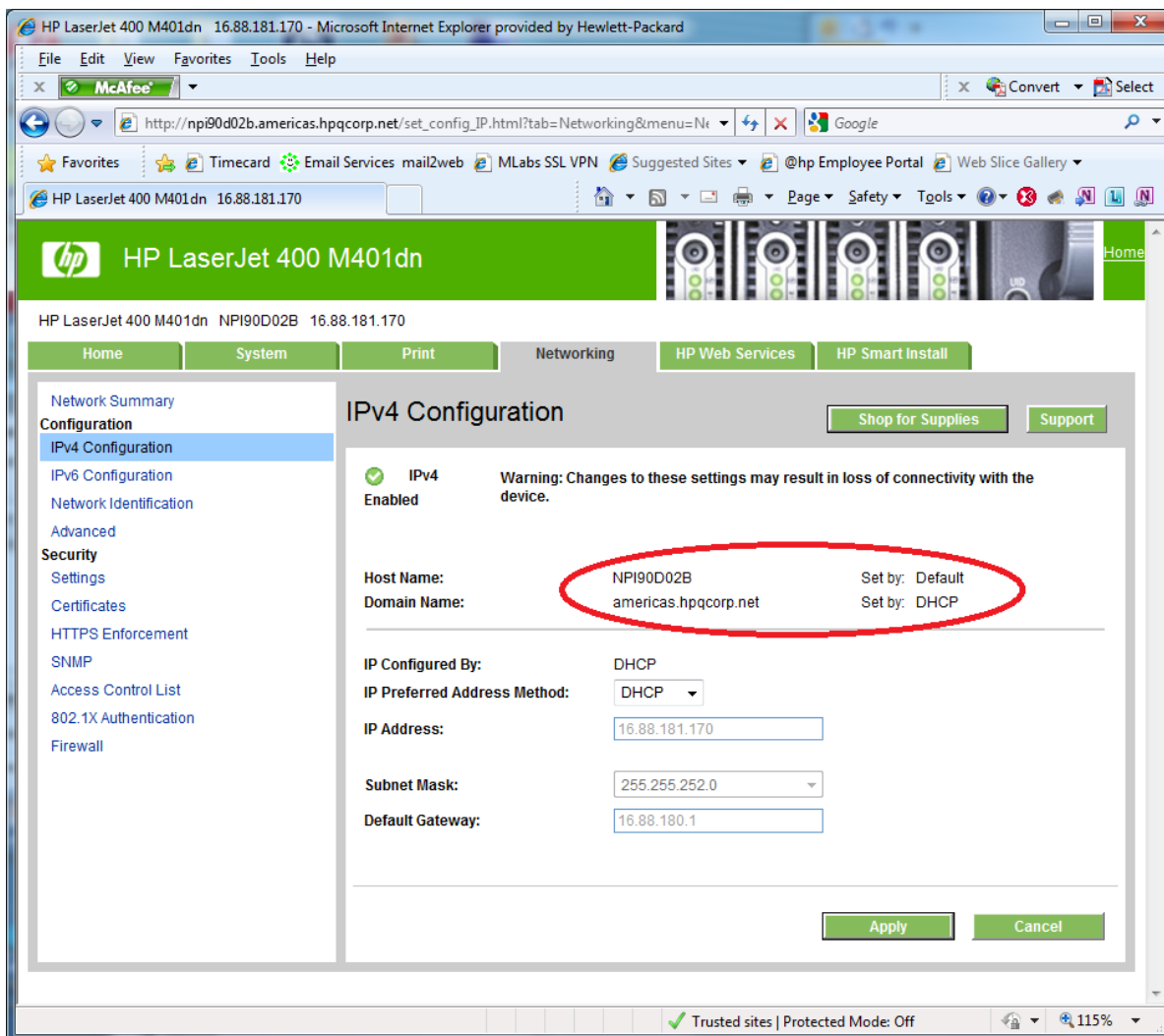
The user friendly interface provides most of the functions needed to manage certificates. To generate a CSR, choose the "Create CSR" option:



The following form will be presented:

Detailed help for each topic is provided on the right hand side of the window.

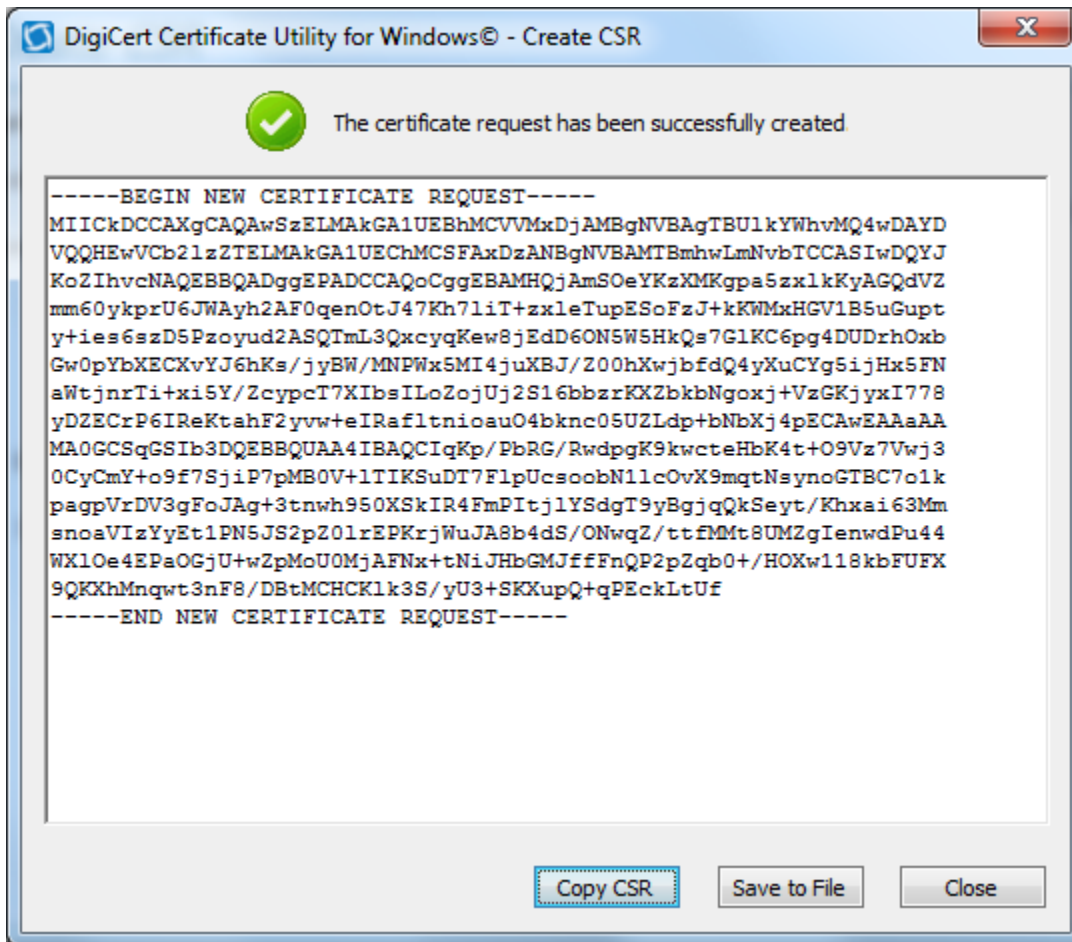
For a printer, choose the “SSL” certificate type and “2048” for the “Key Size”. The “Common Name” is the name that will be used to access the printer. Most often, this will be the Fully Qualified Domain Name (FQDN). This is a combination of the Host Name followed by the Domain Name. In the following example, the FQDN would be: “NPI90D02B.americas.hpqcorp.net”



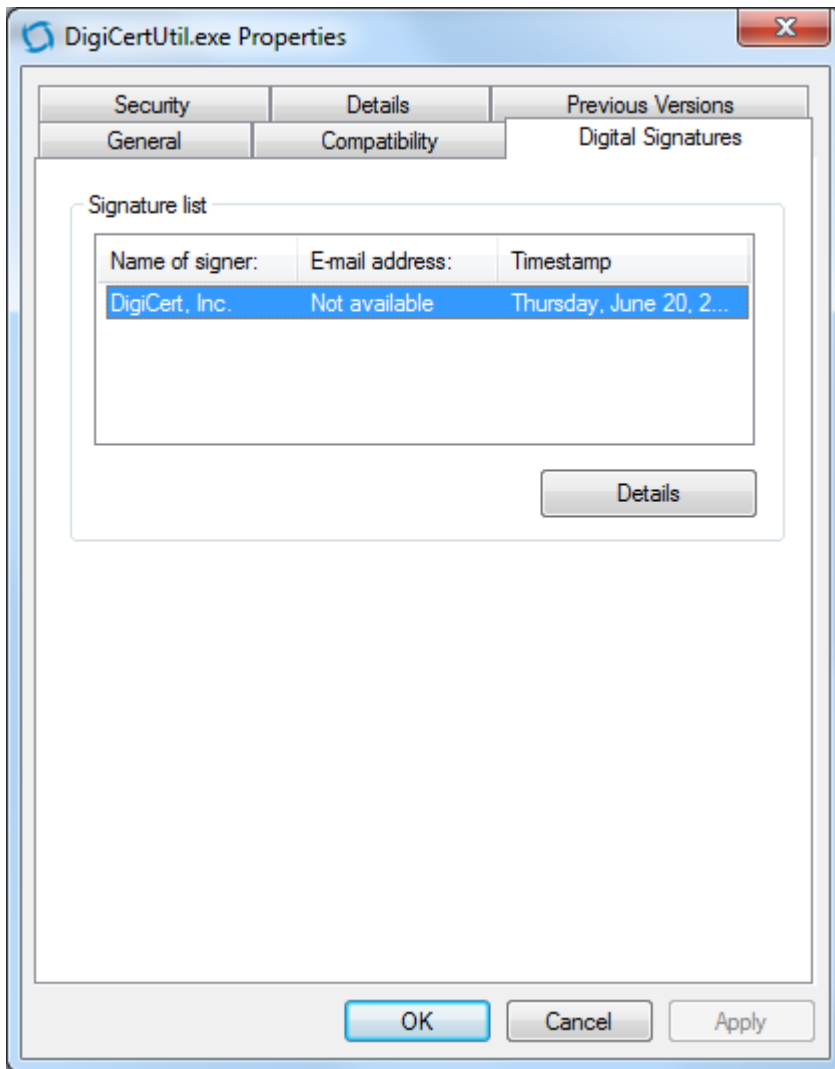
Less often, printers are accessed using just the Host Name (e.g.: "NPI90D02B"). And, sometimes printers are accessed using the IP address (16.88.181.170 in this example). The most important factor in setting the Common Name is to make sure that it doesn't change. If the Common Name changes, then the certificate will no longer be valid. A new certificate will need to be obtained. So, if the printer is configured by DHCP, then it's probably not a good idea to use the IP address (since it will change periodically).

Part of value of a certificate is having a trustworthy and well respected agency (the CA) vouch for your device (the printer). They "certify" that the printer belongs to you and that you are a real company/person and not just someone spoofing a printer for illicit purposes (i.e. to obtain confidential information, etc.). So, providing accurate information is vital to the process of obtaining a certificate. The best CAs will verify all of it before issuing a certificate.

Once the correct information is entered, the "Generate" button is pressed and a CSR is created. This is the CSR:



The utility also stores away the private key for future reference (it will be needed after the certificate is issued). If you use this method, be sure that the program has a valid code signature and is from a reputable source. This can be done by examining the “Digital Signatures” tab of the “Properties” dialog (accessed by right-clicking the file name and selecting “Properties”).



Here are some other examples of software that can be used to generate a 2048 bit CSR

- <http://www.trustico.com/ssltools/create/csr-pem/create-a-new-csr-instantly.php>
- <http://www.gogetssl.com/online-csr-generator/>
- <https://certificatesssl.com/ssl-tools/csr-generator.html>

Method 2 – OpenSSL

The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL toolkit and its related documentation.

A Windows based version of the OpenSSL toolkit can be obtained through the link on this page:

<http://www.openssl.org/related/binaries.html>

1. Download and install the appropriate Visual C++ 2008 Redistributables (x32 or x64 – depending on your system)
2. Download and install the appropriate version of OpenSSL (x32 or x64 – depending on your system).
3. Copy openssl.cfg from C:\OpenSSL-Win64\bin (or C:\OpenSSL-Win32\bin) to C:\usr\local\ssl and rename it to openssl.cnf

This is a command line utility (run from the Command Prompt) which will generate a CSR. It needs to be executed from the same directory that it is installed in.

```
Administrator: Command Prompt
C:\>cd C:\OpenSSL-Win64\bin
C:\OpenSSL-Win64\bin>openssl req -new -newkey rsa:2048 -nodes -out NPI90D02B_yourdomain_com.key -subj "/C=US/ST=Your State/L=Your City/O=Your Company Inc./OU=Sales"
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'NPI90D02B_yourdomain_com.key'
-----
C:\OpenSSL-Win64\bin>
```

It can be complicated and confusing to try and figure out all the details of the command line for OpenSSL. So, DigiCert has created the "OpenSSL CSR Wizard" which will generate the proper command line from the input provided:

OpenSSL CSR Creation

OpenSSL CSR Wizard The fastest way to create your CSR for Apache (or any platform using OpenSSL)

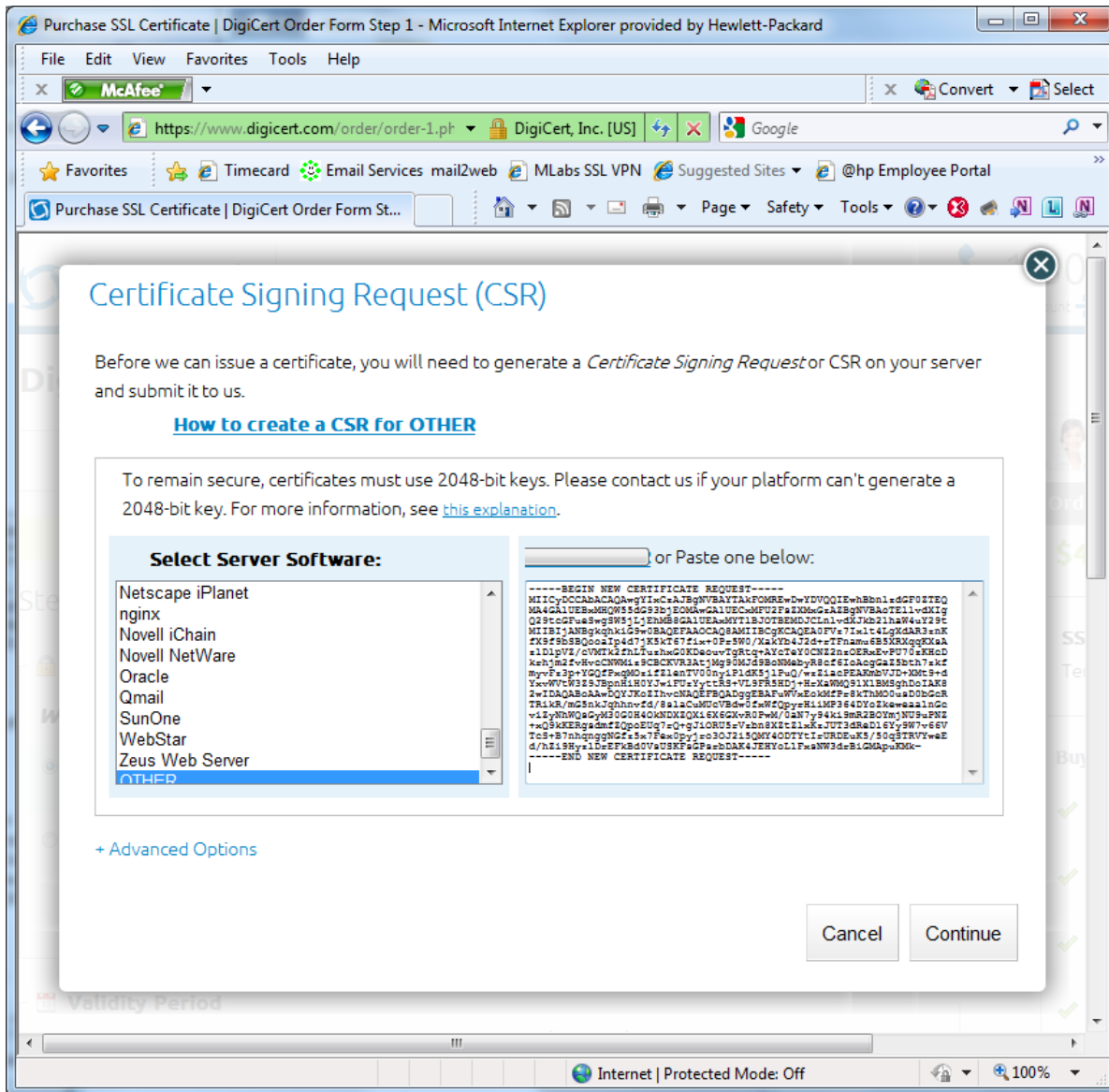
Fill in the details, click Generate, then paste your customized OpenSSL CSR command into your terminal.

Certificate Details	Information
Common Name: <input type="text" value="NPI90D02B.yourdomain.com"/> Organization: <input type="text" value="Your Company, Inc."/> Department: <input type="text" value="Sales"/> City: <input type="text" value="Your City"/> State: <input type="text" value="Your State"/> Country: <input type="text" value="USA"/> Key Size: <input type="text" value="2048 (recommended)"/>	Now just copy and paste this command into a terminal session on your server. Your CSR will be written to NPI90D02B_yourdomain_com.csr. <pre>openssl req -new -newkey rsa:2048 -nodes -out NPI90D02B_yourdomain_com.csr -keyout NPI90D02B_yourdomain_com.key -subj "/C=US/ST=Your State/L=Your City/O=Your Company Inc./OU=Sales/CN=NPI90D02B.yourdomain.com"</pre>
<input type="button" value="Generate"/>	

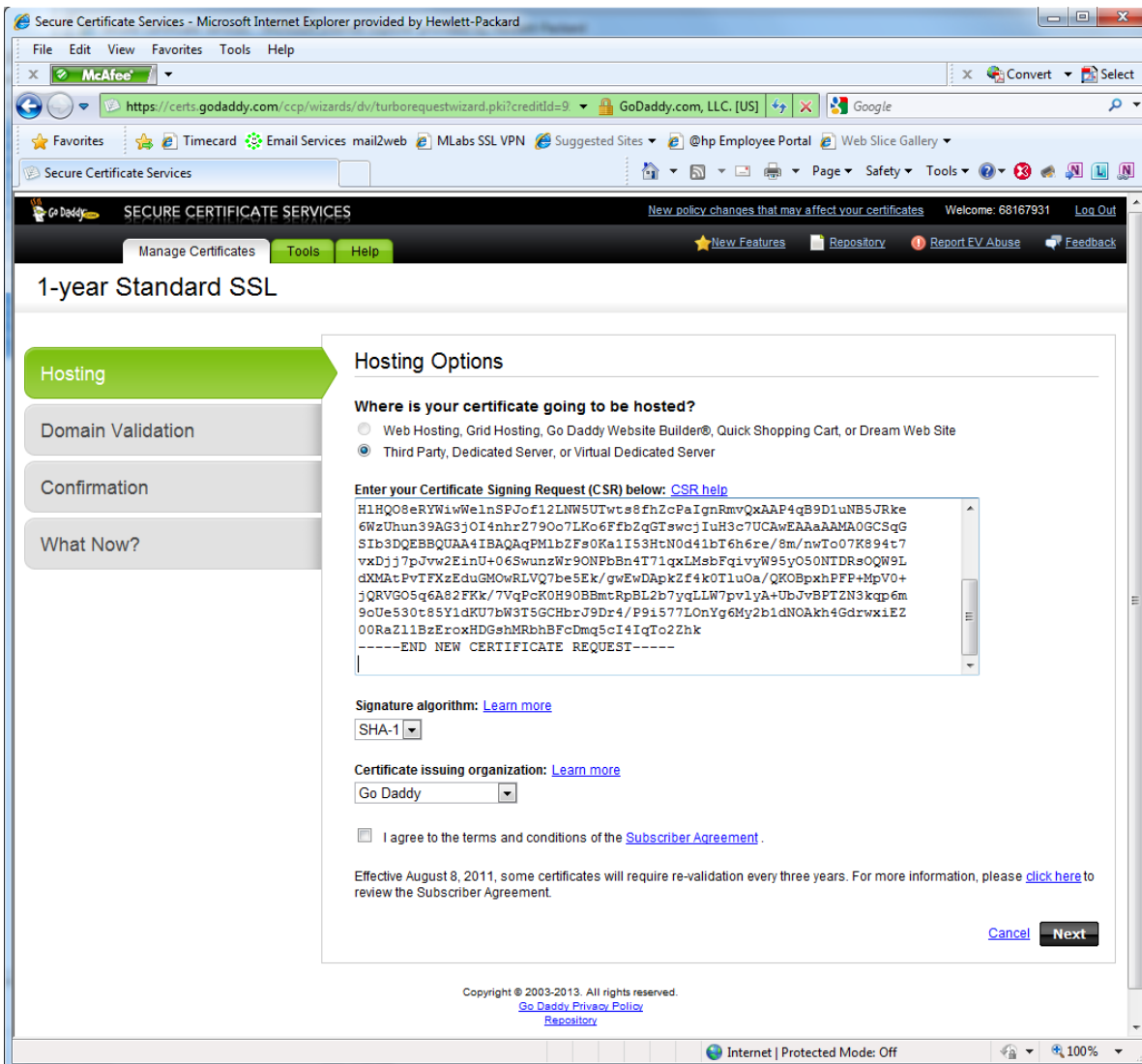
The command shows up in the box on the right. It can be copied and pasted into the command line. In this example, the CSR will be put into a file named: NPI90D02B_yourdomain_com.csr. The private key will be put into a file named: NPI90D02B_yourdomain_com.key.

Obtaining a certificate from the CA

This step of the process the same no matter how the CSR is generated. All of the top CAs will have a page on their web site which facilitates submission. Here is an example:



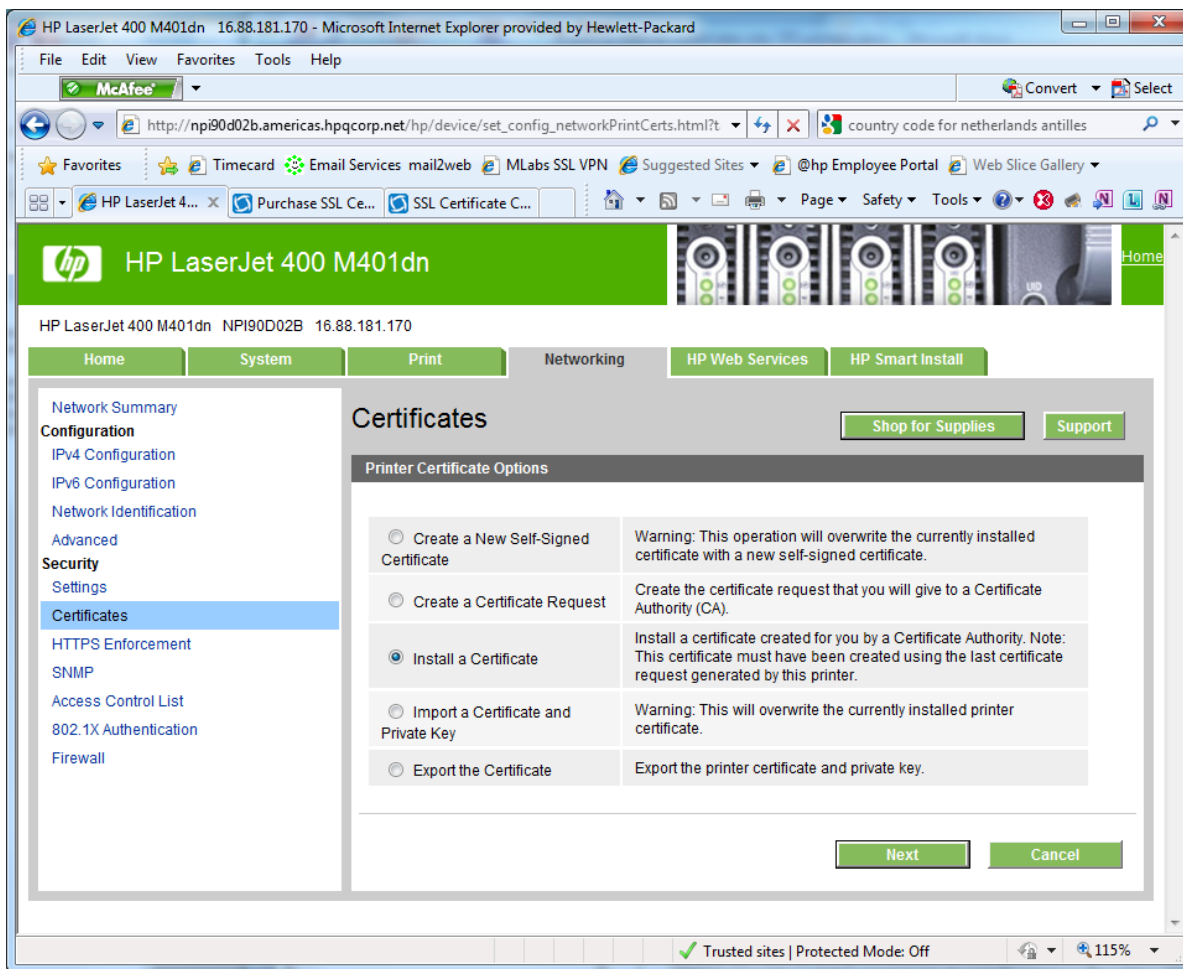
Here is another example:



In both cases, the CSR is copied directly to the text box provided on the page. Assuming everything goes well, the certificate will be provided by email or available for download. It will be a text file with encrypted data that the printer will use once the certificate is installed. It can take one of these three formats:

1. Cryptographic Message Syntax Standard ((.P7B, .P7R or .SPC)
The PKCS #7 format supports storage of certificates and all certificates in the certification path.
2. DER-encoded binary X.509 (.DER, .CER, or .CRT)
The Distinguished Encoding Rules (DER) format supports storage of a single certificate. This format does not support storage of the private key or certification path.
3. Base64-encoded X.509 (.CER or .CRT)
The Base64 format supports storage of a single certificate. This format does not support storage of the private key or certification path.

Here's a typical example:



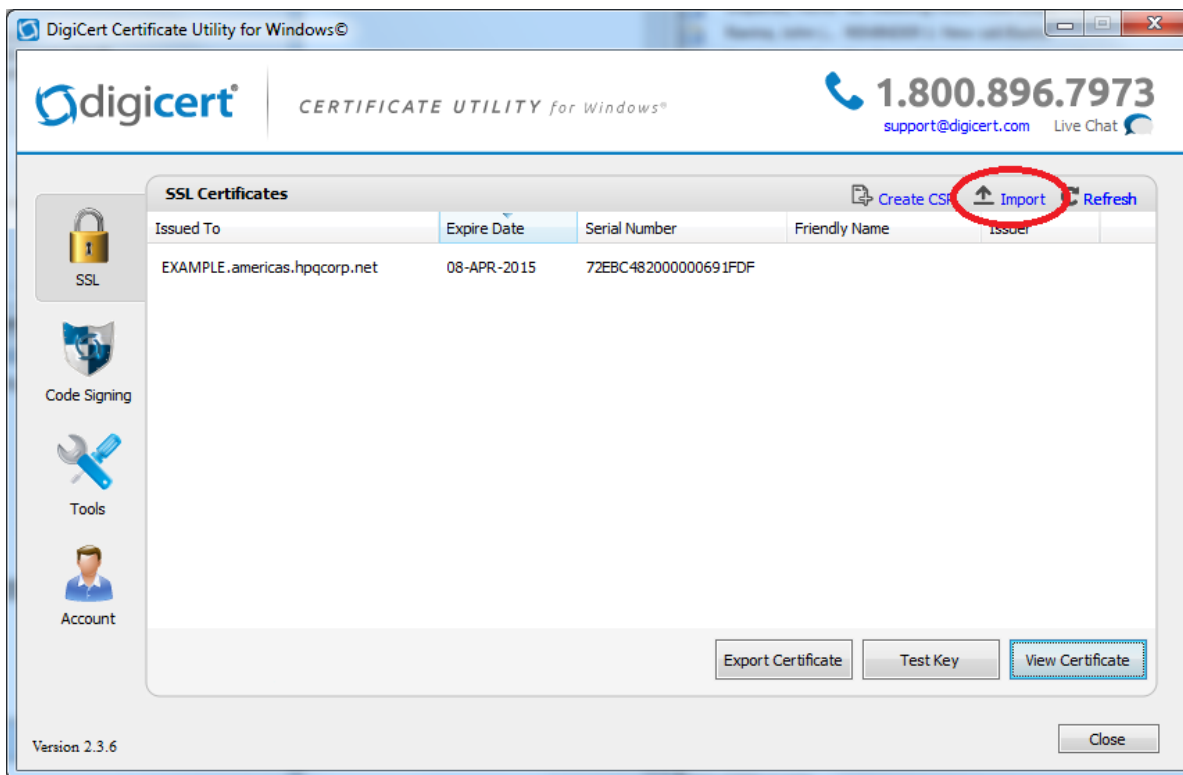
This option will not appear if the CSR was generated by one of the alternate methods. If it is visible (from a previous attempt to generate a CSR), then it will only work with the certificate which resulted from the most recent printer-generated CSR. It will not work with certificates generated by one of these alternate methods. Instead, the certificate must be converted to the “Personal Information Exchange” format (PKCS #12 , .PFX, or .P12) and installed using the “Import a Certificate and Private Key” option.

Converting the Certificate to the Personal Information Exchange (.PFX) format

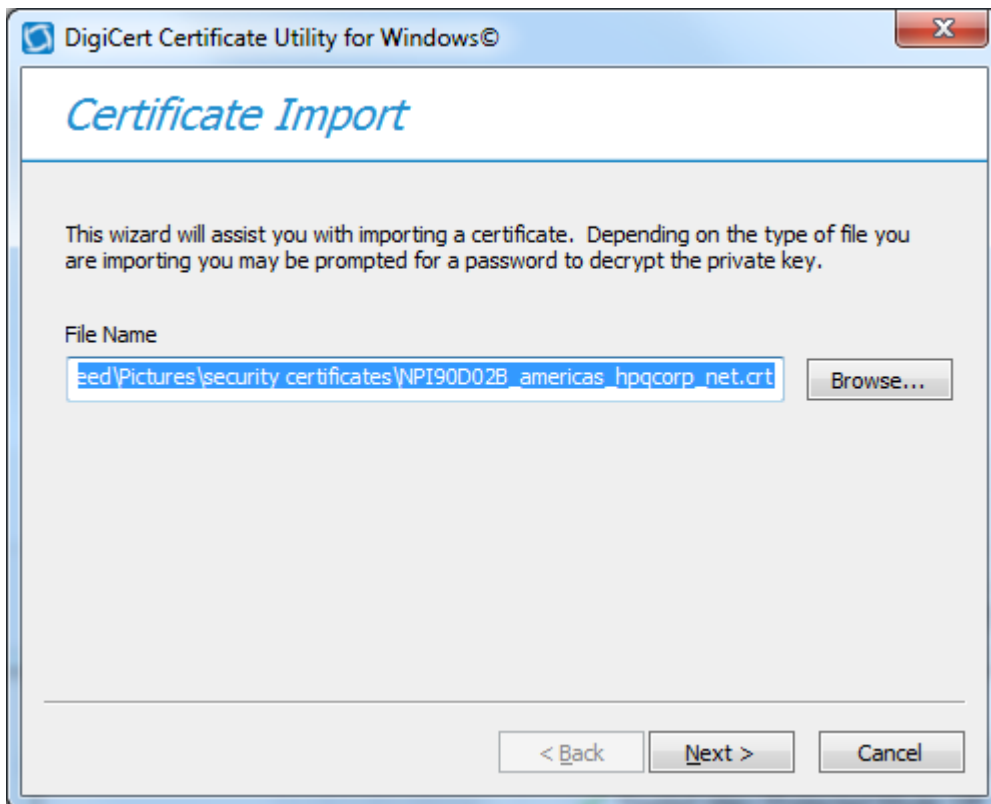
If a certificate was obtained using a CSR which was not generated by the printer, then it cannot be installed directly into the printer. It must first be converted to the PKCS #12 , .PFX, or .P12 format. Then the “Import” option can be used to transfer the certificate and private key to the printer. Most certificate management programs can provide this function. DigiCert’s Certificate Utility is shown here for example purposes.

Method 1 – Software supplied by the CA

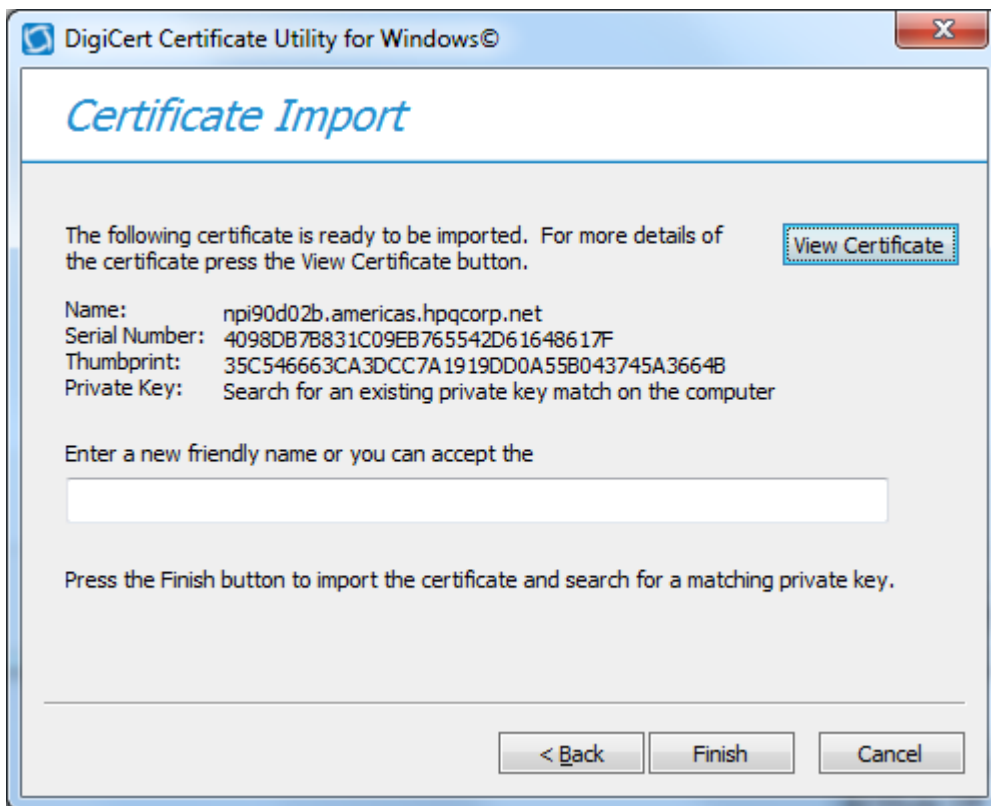
The first step is to select the “Import” option on the main window of the Certificate Utility:



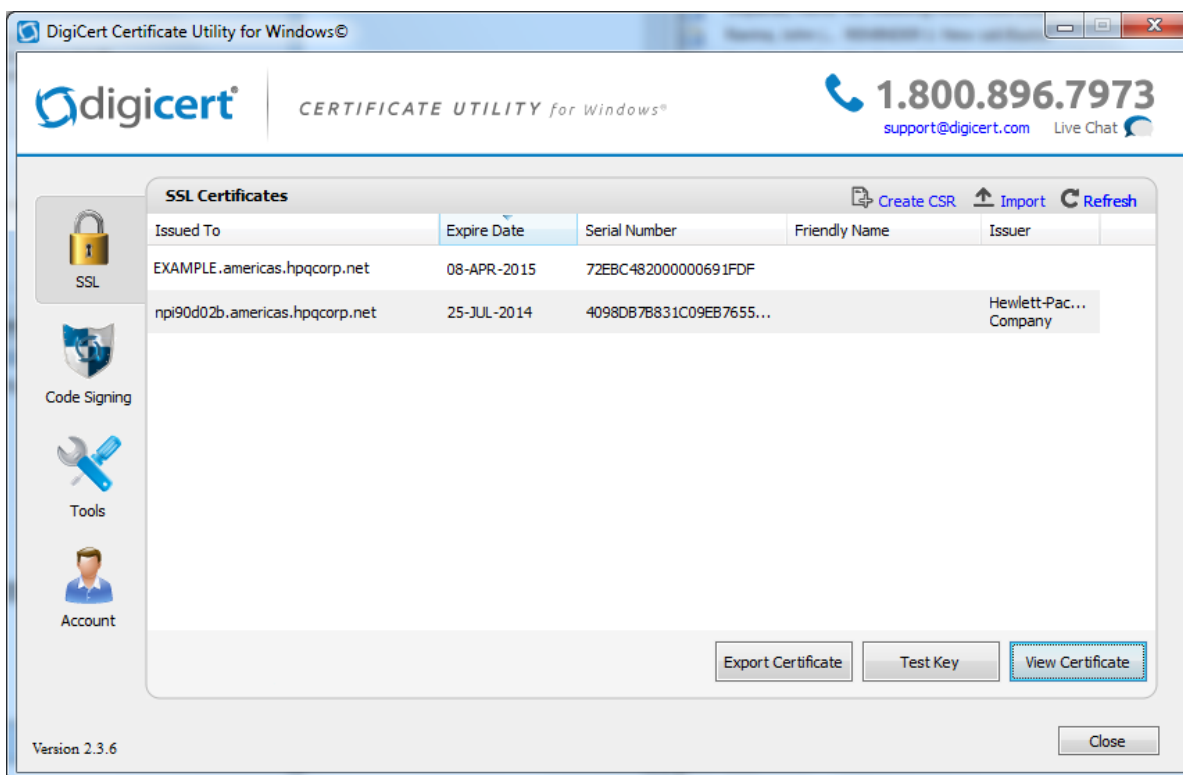
Next, provide the name of the file that contains the certificate:



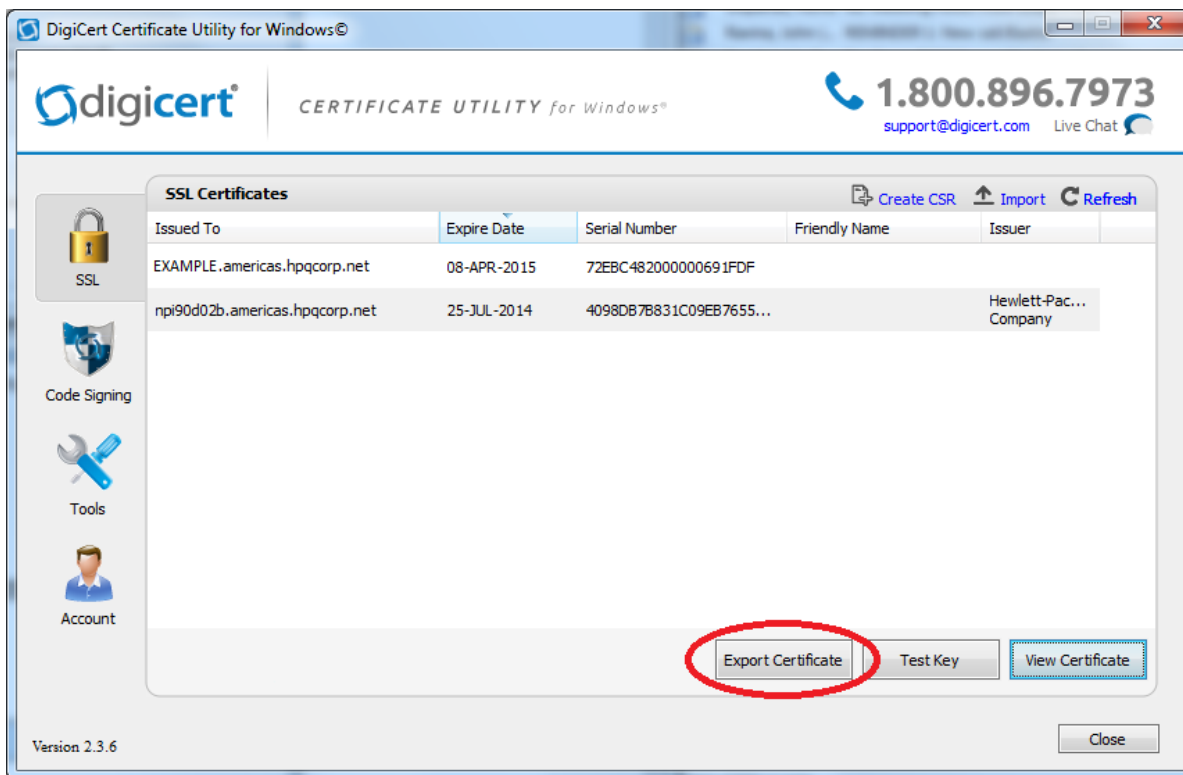
Select the "Finish" button when ready to import the certificate:



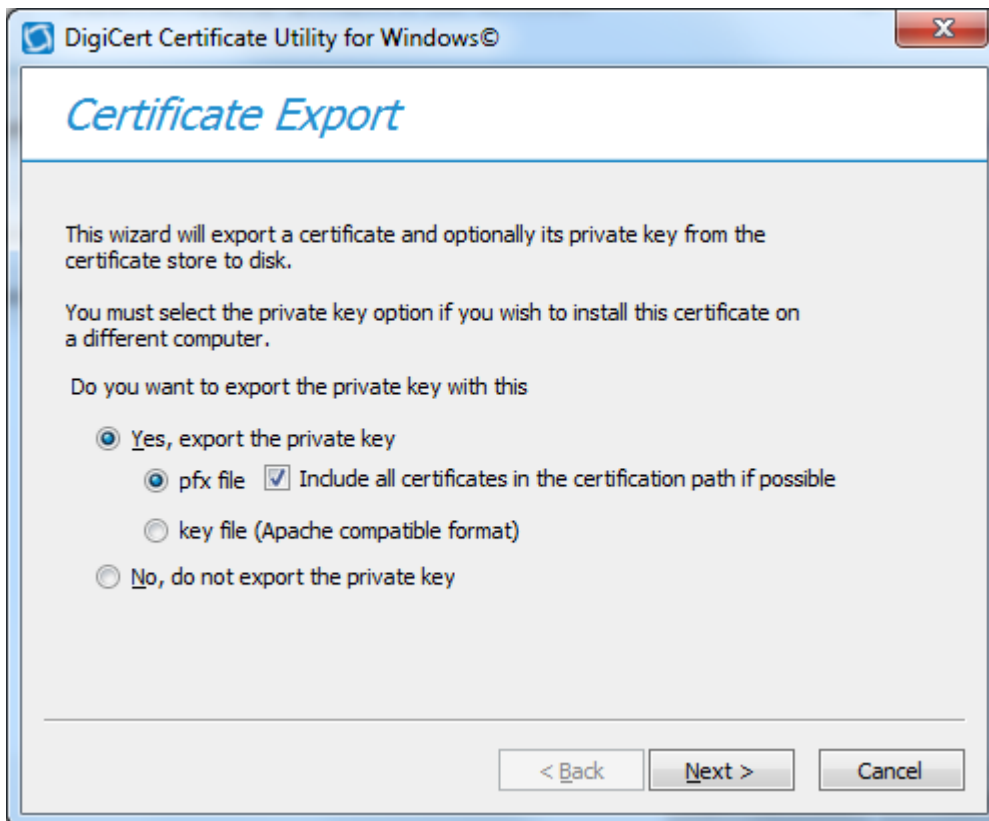
The main screen of the utility will now include the new certificate:



Next, select the “Export Certificate” button on the main window of the Certificate Utility:



and choose "pfx file" option as shown here:



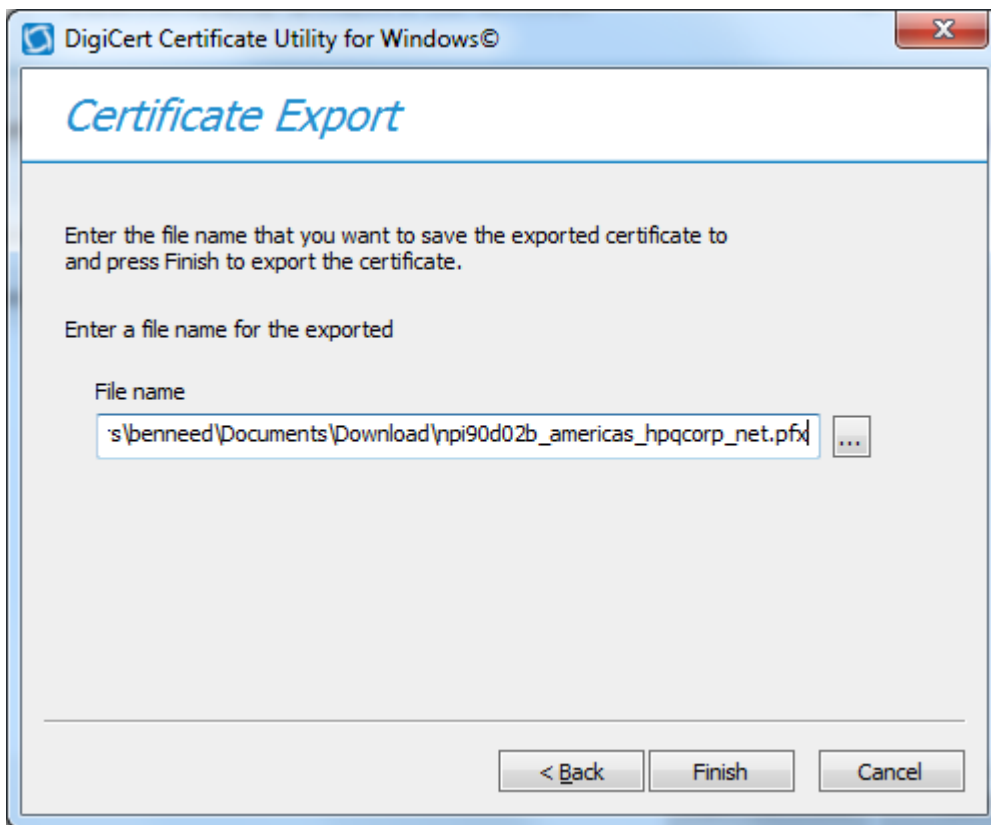
The PFX format is required by the LaserJet printer. It contains everything needed to protect the printer from unauthorized access:

- Certificate
- Public key
- Private key

These are also the three vital components that a hacker needs to circumvent the printer security. So, treat this file with great care. Always store it in a safe and secure location. A password is required to help prevent unauthorized access. Do not share this password with anyone.



Provide a name and location for the .PFX file:



Here are some examples of other software than can be used to create the PFX file:

<http://www.trustico.com/ssltools/convert/pem-to-pkcs12/convert-pem-to-pkcs12.php>

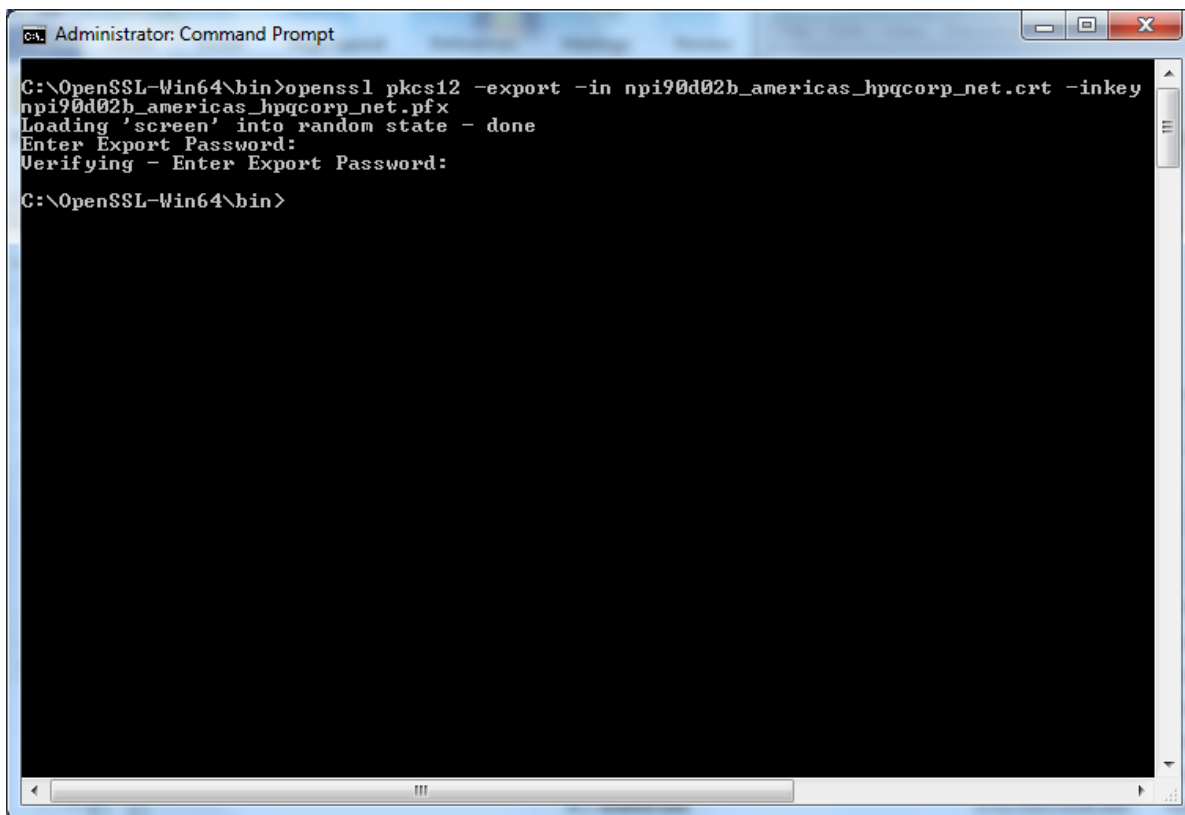
<https://certificatesssl.com/ssl-tools/convert-certificate.html>

Method 2 - OpenSSL

OpenSSL can also be used to create the PFX file that can be imported into the printer. Use the following command:

```
openssl pkcs12 -export -in <cert-file-name.ext> -inkey <key-file-name.ext> -out <export-file-name>.pfx
```

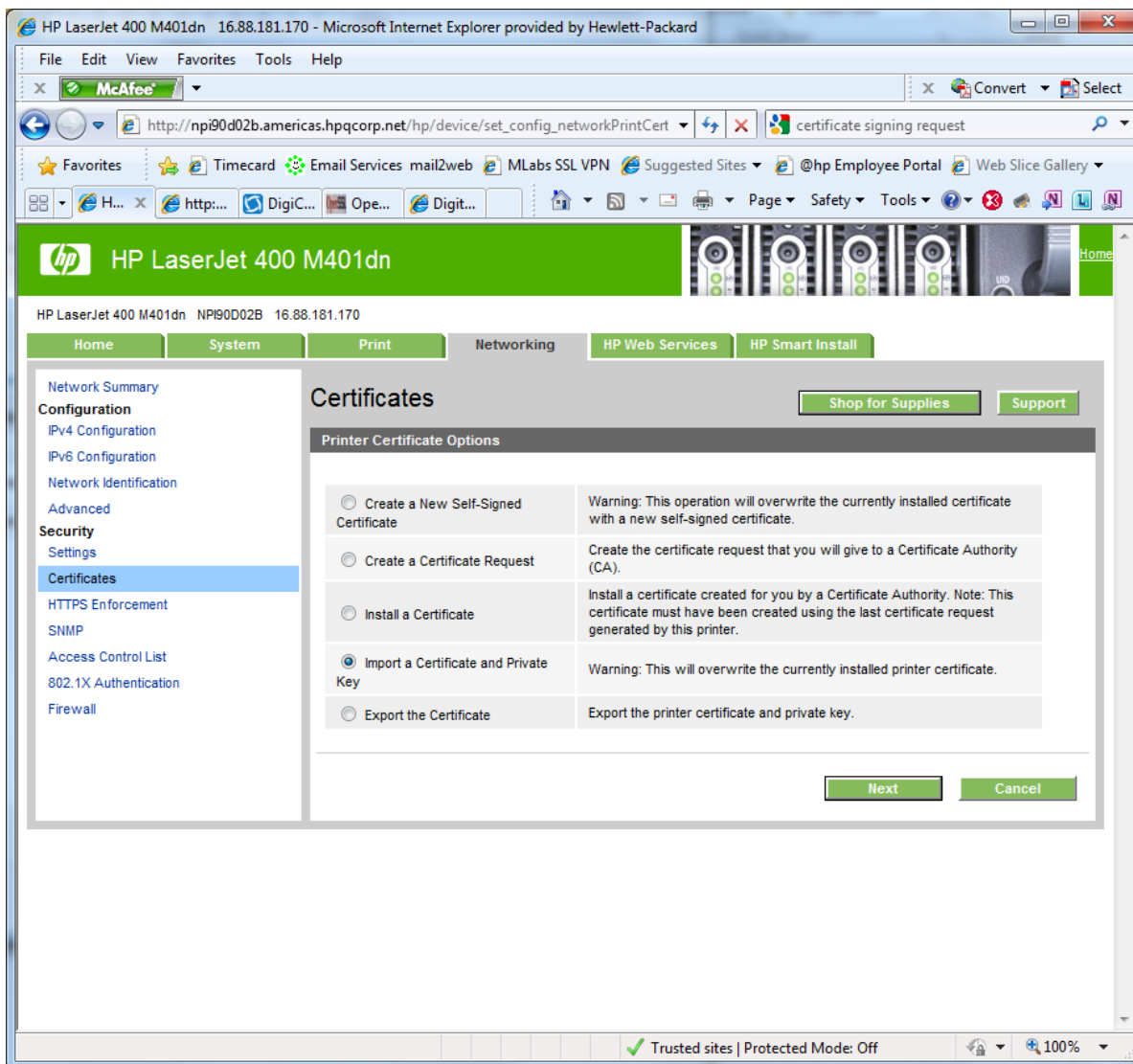
Substitute the items contained in "<...>" with the appropriate file names for the certificate, the private key, and the output PFX file. This command will prompt for a password to protect the private key (just like the DigiCert utility). This password will be required when importing the certificate into the printer. Here's an example of how it works:



```
Administrator: Command Prompt
C:\OpenSSL-Win64\bin>openssl pkcs12 -export -in npi90d02b_americas_hpgcorp_net.crt -inkey
npi90d02b_americas_hpgcorp_net.pfx
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:
C:\OpenSSL-Win64\bin>
```

Installing the new certificate

The certificate is now in a format that can be accepted by the printer. From the “Printer Certificate Options” page on the printer EWS, choose the “Import a Certificate and Private Key” option and select “Next”:



Provide the filename for the .PFX file and the password that was used when the file was originally created. Select "Finish".

HP LaserJet 400 M401dn 16.88.181.170 - Microsoft Internet Explorer provided by Hewlett-Packard

File Edit View Favorites Tools Help

McAfee Convert Select

http://np190d02b.americas.hpqcorp.net/hp/device/set_config_networkCertsImp certificate signing request

Timecard Email Services mail2web MLabs SSL VPN Suggested Sites @hp Employee Portal Web Slice Gallery

HP LaserJet 400 M401dn

HP LaserJet 400 M401dn NP190D02B 16.88.181.170

Home System Print Networking HP Web Services HP Smart Install

Network Summary
Configuration
IPv4 Configuration
IPv6 Configuration
Network Identification
Advanced
Security
Settings
Certificates
HTTPS Enforcement
SNMP
Access Control List
802.1X Authentication
Firewall

Certificates

Shop for Supplies Support

Import a Certificate and Private Key

Enter the name of the file that contains the certificate and private key. You must provide the password that was used to encrypt the private key.

The file format must be PKC S#12 encoded (.pfx).

File Name: * C:\Users\benneed\Pictures\security certificates Browse...

Password: *

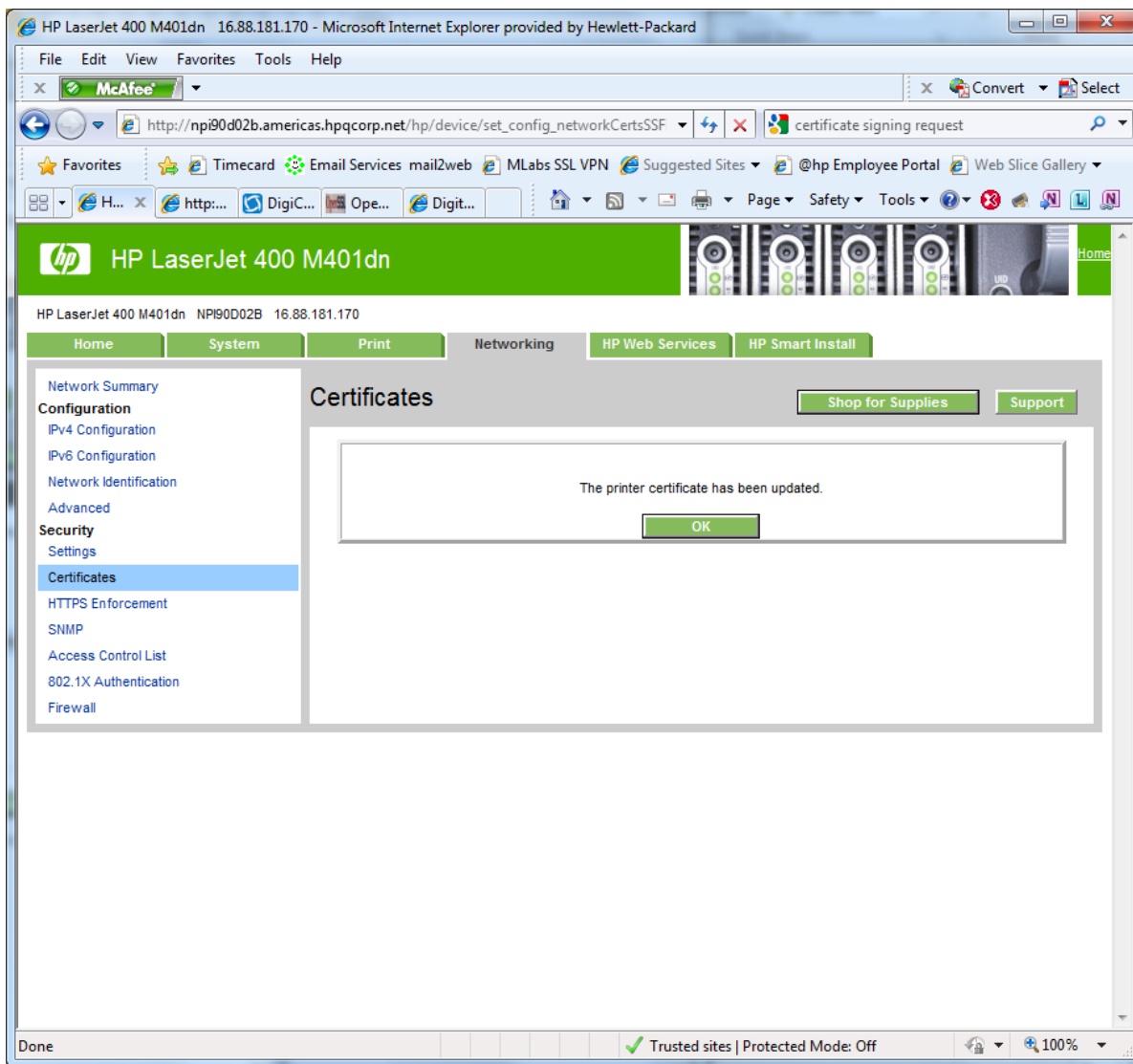
Mark private key as exportable.

* required field

Finish

Back Cancel

Trusted sites | Protected Mode: Off 100%



Select "OK" to return to the main Certificates screen. To verify that the new certificate has been installed, select the "View" button:

The screenshot shows the HP LaserJet 400 M401dn web interface in Microsoft Internet Explorer. The browser address bar shows the URL: http://np190d02b.americas.hpqcorp.net/hp/device/set_config_networkViewPrint. The page title is "HP LaserJet 400 M401dn". The interface includes a navigation menu with tabs for Home, System, Print, Networking, HP Web Services, and HP Smart Install. The "Certificates" tab is selected, and the "Certificates" page is displayed. The page shows the following information:

- Printer Certificate Options**
- Version: 3 (0x2)
- Serial Number: 40:98:db:7b:83:1c:09:eb:76:55
- Signature Algorithm: sha1WithRSAEncryption
- Issuer: Hewlett-Packard Private Class 2 Certification Authority
- Validity: Issued On: 2013-07-25 00:00 UTC, Expires On: 2014-07-25 23:59 UTC
- Subject: np190d02b.americas.hpqcorp.net
- Public Key: Public Key Algorithm: rsaEncryption RSA Public Key: (2048 bit) Modulus (2048 bit): 00:c5:23:b5:ad:76:0c:3d:ff:5f:05:fd:f6:ee:5a:dd:ab:79:ff:31:30:17:05:1c:57:a7:77:58:1b:f0:0a:d1:99:f4:06:fe:70:e9:ae:40:2f:c9:b4:58:ba:9c:
- Extensions: Authority Key Identifier: : keyid:37:ED:F7:15:79:2D:30:A5:98:9A:75:B6:5C:37:E3:88:EA:11:6A:D5, Subject Key Identifier: : 97:60:E1:F2:EE:C7:85:FD:4D:C2:FF:AE:65:CC:A1:7E:42:7B:13:2A, Key Usage: : critical TLS Web Server Authentication, TLS Web Client Authentication, E-mail Protection

Applicable Products

HP LaserJet Pro 200 color Printer M251n – CF146A
HP LaserJet Pro 200 color Printer M251nw – CF147A
HP TopShot LaserJet Pro M275 MFP – CF040A
HP LaserJet Pro 200 color MFP M276n – CF144A
HP LaserJet Pro 200 color MFP M276nw – CF145A
HP LaserJet Pro 400 color Printer M451dn – CE957A
HP LaserJet Pro 400 color Printer M451dn – CE957A
HP LaserJet Pro 400 color Printer M451dn – CE957A
HP LaserJet Pro 400 color Printer M451dw – CE958A
HP LaserJet Pro 400 color Printer M451nw – CE956A
HP LaserJet Pro 300 color MFP M375nw – CE903A
HP LaserJet Pro 400 color MFP M475dn – CE863A
HP LaserJet Pro 400 color MFP M475dw – CE864A
HP LaserJet Pro 400 Printer M401a – CF270A
HP LaserJet Pro 400 Printer M401d – CF274A
HP LaserJet Pro 400 Printer M401dn – CF278A
HP LaserJet Pro 400 Printer M401dne – CF399A
HP LaserJet Pro 400 Printer M401dw – CF285A

HP LaserJet Pro 400 Printer M401n – CZ195A
HP LaserJet Pro 400 MFP M425dn – CF286A
HP LaserJet Pro 400 MFP M425dw – CF288A

For more information

To read more about this issue, go to: hp.com/support

Call to action

Please contact your HP representative or visit: hp.com/go/product

hp.com/go/support

Current HP driver, support, and security alerts
delivered directly to your desktop

© 2016 Copyright HP Development Company, L.P. 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.

Trademark acknowledgments, if needed.

4AA4-xxxxENW, Created Month 2013

