

HISPDirect Certificate Request and Identity Process

The HISPDirect Security Certificate and Subdomain process is very easy to accomplish when you follow the step-by-step instructions provided below. Step 1 will walk you through the process of completing the certificate request form. Step 2 will walk you through the process of completing the required documentation by the Certificate Authority (DigiCert).

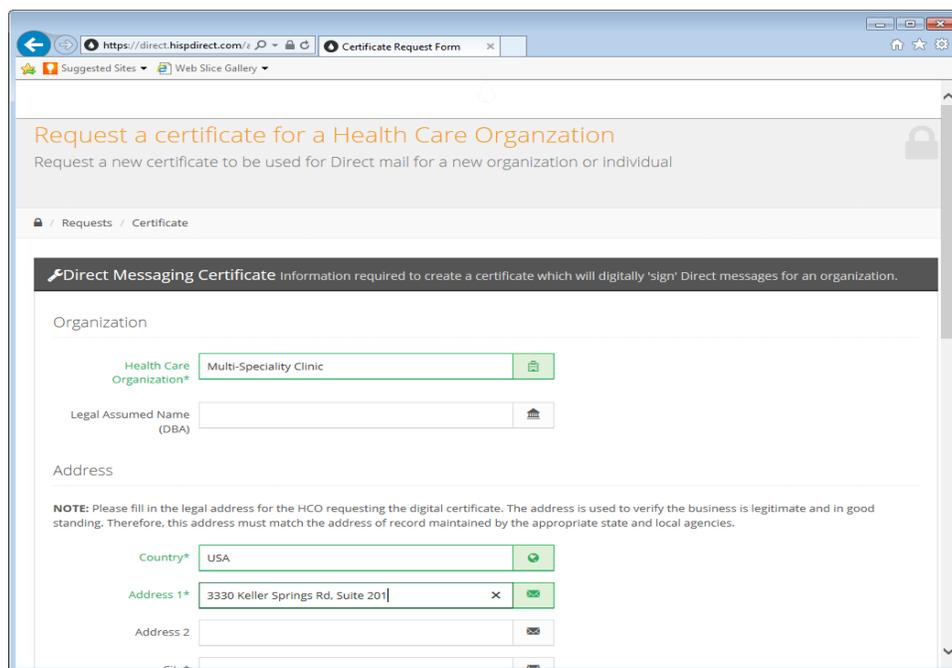
Step 1: Request DigiCert Certificate and HISPDirect Subdomain

Use this process to request the DigiCert certificate and HISPDirect subdomain. Nitor will process your subdomain request, and send your security certificate request to DigiCert. Then, DigiCert will send an email to your authorized representative. This will take approximately one business day.

1. Select the following link to access the Nitor website.

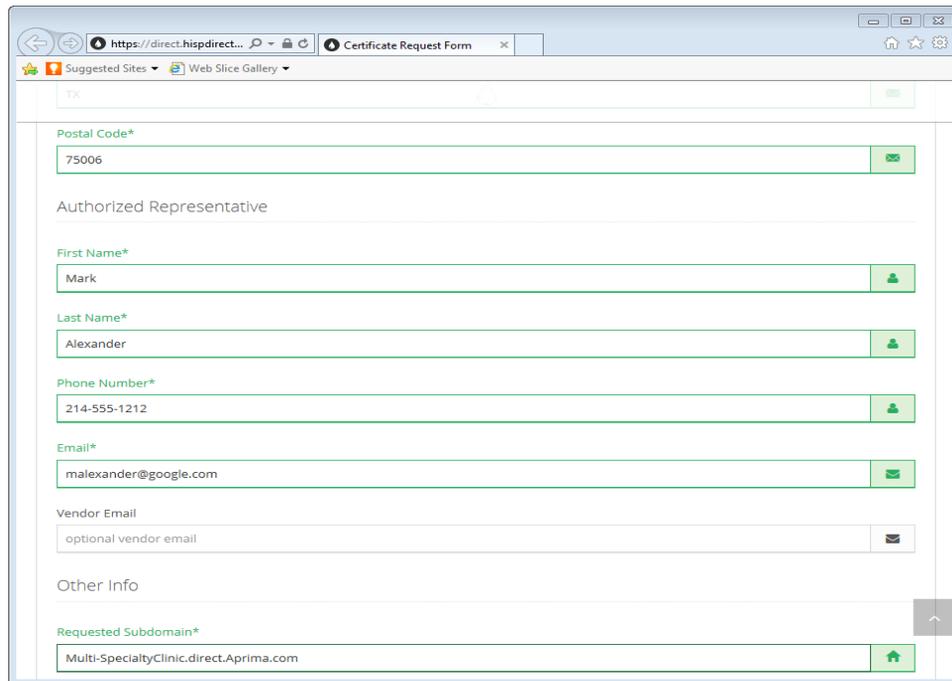
<https://direct.hispdirect.com/adminportal/requestAR.php>

2. Identify your practice.

A screenshot of a web browser displaying the 'Certificate Request Form' on the HISPDirect website. The browser's address bar shows 'https://direct.hispdirect.com/'. The page title is 'Certificate Request Form'. The main heading is 'Request a certificate for a Health Care Organization' with a sub-heading 'Request a new certificate to be used for Direct mail for a new organization or individual'. Below this is a breadcrumb trail: 'Requests / Certificate'. A dark banner reads 'Direct Messaging Certificate Information required to create a certificate which will digitally 'sign' Direct messages for an organization.' The form is divided into sections: 'Organization' with a dropdown menu for 'Health Care Organization*' set to 'Multi-Specialty Clinic' and an empty 'Legal Assumed Name (DBA)' field; and 'Address' with a 'NOTE' about legal address requirements, a dropdown for 'Country*' set to 'USA', and an 'Address 1*' field containing '3330 Keller Springs Rd, Suite 201'. There are also empty fields for 'Address 2' and 'City, State, ZIP'.

- a. In the Health Care Organization field, enter the name of the legal business entity that is your practice.
- b. If appropriate, enter a name in the Legal Assumed Name (DBA) field.
- c. In the Address section, enter the physical address of your practice. This must include the country, street address, city, state, and ZIP code.

3. Scroll down to identify your practice authorized representative.



The screenshot shows a web browser window with the address bar displaying "https://direct.hispdirect...". The page title is "Certificate Request Form". The form contains the following fields:

- Postal Code*: 75006
- Authorized Representative section:
 - First Name*: Mark
 - Last Name*: Alexander
 - Phone Number*: 214-555-1212
 - Email*: malexander@google.com
 - Vendor Email: optional vendor email
- Other Info section:
 - Requested Subdomain*: Multi-SpecialtyClinic.direct.Aprima.com

- Enter your First and Last Names.
- Enter your Phone Number.
- Enter your Email address.
- Leave the Vendor Email address field blank.

4. Scroll down to the Other Info section to request your Nitor subdomain.

The screenshot shows a web browser window with the URL <https://direct.hispdirect...> and the page title "Certificate Request Form". The form contains several fields: "Phone Number*", "Email*" (with the value "malexander@gmail.com"), "Vendor Email" (with the value "optional vendor email"), and "Requested Subdomain*" (with the value "@Multi-SpecialtyClinic.direct.Aprima.com"). A "Tip" box is overlaid on the "Requested Subdomain*" field, containing the text: "Fully specify the subdomain that will be in your Direct addresses; as in @<MyPractice>.direct.MyEHR.com". Below the "Requested Subdomain*" field is the "Terms of Service" section, which includes a checkbox for "I Agree" (checked) and a "Submit" button. The footer of the page includes "2013-2015 © Rosetta Health Portal" and "Crafted with ♥ by Nitor Group".

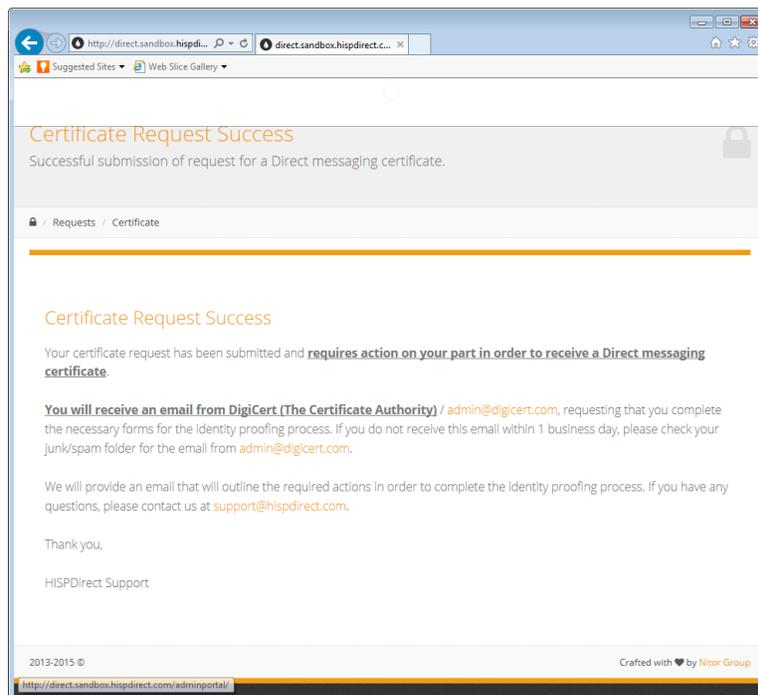
- a. In the Requested Subdomain field, enter the fully qualified domain for your certificate. Include both the subdomain you are requesting to identify your practice and the EHR or vendor domain, as shown below.

@PracticeSubdomain.direct.EHRorVendorname.com

Your practice subdomain name may include the letters (A-Z) and numbers (0-9). You may also include a hyphen (-), but the hyphen cannot be the first or the final character of the subdomain name. The subdomain cannot include any other special characters.

5. Agree to the terms of service and submit your request.
- a. Select the I Agree checkbox.
- b. Select the Submit button.

6. When the certificate request Success message displays, close your browser window.



Step 2: Complete Your Identity Verification

You will receive an email from DigiCert within approximately one business day of requesting your security certificate and HISPDirect subdomain. The email contains a link to a DigiCert website where you can complete some of your identity information. You must also download and print an additional form. You must complete that form, take it to notary public to have the completed form notarized, scan the notarized document, and upload the scanned file to the DigiCert website using the link provided in the email.

IMPORTANT: The link in this email is valid for **only 14 days**. You must complete the documentation and upload it within that 14-day period. Otherwise, the link will expire, and you will need to complete the Request DigiCert Certificate and HISPDirect Subdomain process (above) again in order to get a new email with a new link.

1. Open the email from DigiCert, and select the link to the identity verification site.
2. Your first and last name are prepopulated. Complete the rest of your personal information.

The screenshot shows the DigiCert website's 'Personal Verification' form. The page header includes the DigiCert logo and the tagline 'YOUR SUCCESS IS BUILT ON TRUST'. Below the header is a 'Support' link. The main form is titled 'Personal Verification' and is divided into two columns: 'Personal Information' and 'Government ID Information'. The 'Personal Information' column contains fields for First Name (pre-filled with 'Example'), Last Name, Contact, Telephone* (with a placeholder 'xxx-xxx-xxxx'), Birth Date* (with a placeholder 'mm/dd/yyyy'), Home Address* (with a placeholder 'xxxx-xxxx-xxxx'), City*, State* (a dropdown menu), and Postal Code*. The 'Government ID Information' column contains fields for Photo ID Type* (a dropdown menu), ID Number*, and Expiration Date* (with a placeholder 'mm/dd/yyyy'). Below these fields is a 'Verification Method' section with two radio buttons: 'Online Verification*' (selected) and 'Declaration of Identity Verification*'. The 'Online Verification*' option includes a note: 'This online verification process will ask you a series of questions in an attempt to verify your identity. If you select this option please be prepared to answer questions pulled from your credit history. To start the process you will be required to enter your social security number.' The 'Declaration of Identity Verification*' option includes a note: 'This Declaration of identity verification process includes downloading a document and having it signed by a notary or trusted agent.' At the bottom of the form is a blue 'NEXT STEP' button. The footer of the page contains the DigiCert logo, links for Terms of Use, Money Back Guarantee, Privacy Policy, Legal Resources, Newsroom, and Site Map, and a copyright notice: '© 2002-2014 DigiCert, Inc. All Rights Reserved. DigiCert, DigiCert Portal, and DigiCert are trademarks or registered trademarks of DigiCert, Inc. in the USA and elsewhere. All other trademarks displayed on this website are the exclusive property of their respective owners.'

3. Scroll to the bottom, and either:
 - Select the Online Verification radio button to complete the process online. This is recommended.
 - Select the Declaration of Identity Verification radio button to complete the paper verification process. This is not recommended as it can take several days (or more) to complete.
4. Select the Next Step button. Then use the process below for the method you have selected.

Perform the Online Verification Process

The online verification process is the preferred process because it avoids the delays inherent in the paper declaration process. You will perform this process if you selected the Online Verification radio button on the DigiCert Personal Verification page.

This process is very similar to identity proofing processes that are commonly used for such things as applying for or renewing a driver's license, applying for loan or credit card, and being hired by a new employer. You will be asked several questions that are generated from your credit history and other sources, such as employment and address history. Your correct answers to these questions confirm your identity.

1. Enter your Social Security number.

Personal Verification

You have selected to use this online identity validation. If you would rather verify your identity through a process using a Declaration of Identity form please [click here](#).

Important Instructions Please Read

You will have 5 minutes to fill out the form on the next page.
After two failed attempts the online validation option will no longer be available.

* Social Security Number

Terms of Service

AUTHORIZATION

DigiCert, Inc. ("DigiCert") issues X.509 v3 digital certificates ("Certificates") to customers of the health information service provider providing this authorization form to you ("HISP"). By accepting this authorization, you agree, on behalf of each Certificate subject you represent ("Applicant"), that HISP and DigiCert may provide, on Applicant's behalf, certain Certificate-related duties that are normally reserved for Certificate subjects. These tasks include managing keys, registering devices, authenticating personnel with DigiCert and its Certificate systems, and installing, configuring, and managing issued Certificates. For purposes of this authorization "you" may be the medical professional, office manager, sponsor, or other trusted agent approved by Applicant to enter into agreements on behalf of Applicant. By checking "I Agree", Applicant hereby agrees and authorizes HISP and DigiCert as follows:

I have read and agree to the terms above

NEXT STEP

2. Select the checkbox for "I have read and agree to the terms above."
3. Select the Next Step button.
4. The next page will present you with several multiple choice questions. Select the correct answer for each question.
5. Select the Done button to complete the process.
6. Close the browser window. DigiCert will process your request.

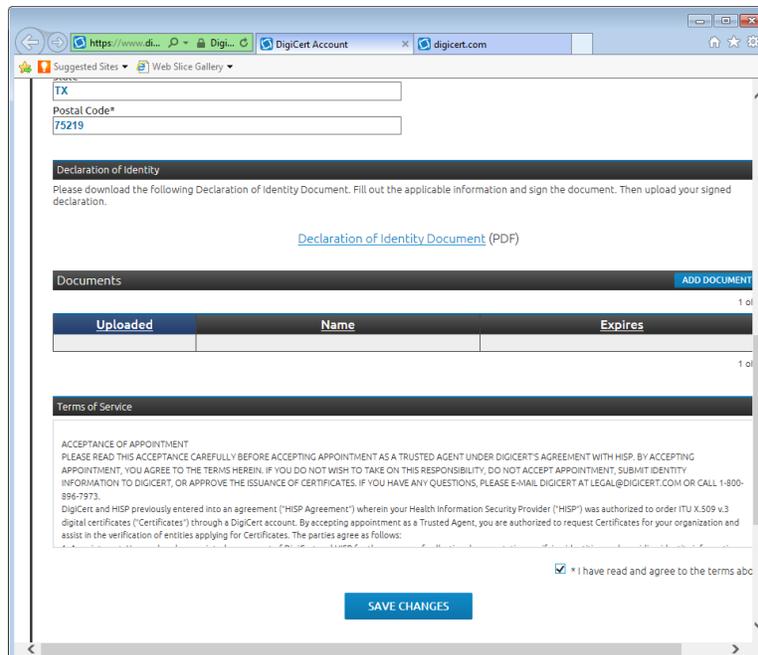
DigiCert will then issue your security certificate to Nitor, and Nitor will enable your Direct message subdomain. When you receive notification that the subdomain is enabled, you may begin creating Direct message addresses for your providers. Instructions for creating Direct message addresses are included on page 10 of the *Direct Messaging Setup for Nitor* document.

Perform the Declaration of Identity Verification Process

Perform this process if you selected the Declaration of Identity Verification radio button on the DigiCert Personal Verification page. In this process, you will complete, and then download and print the Declaration of Identity Document. Then, you must have the printed documented notarized. Finally, you must scan the notarized document and upload the file to the DigiCert site.

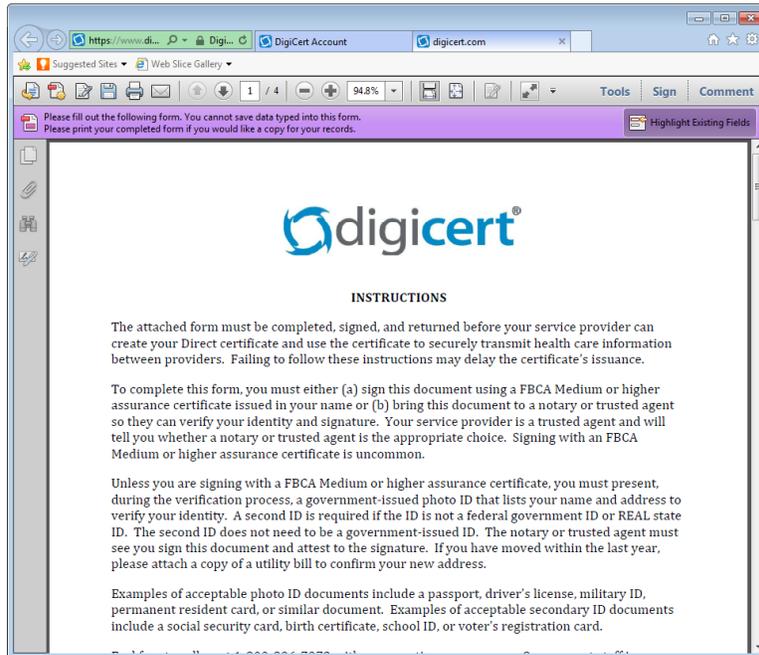
You must complete this process in a timely manner. To upload your scanned notarized document, you must access the DigiCert site using the link in the email you received from DigiCert. The link in that email is valid for **only 14 days**.

1. Select the Declaration of Identity Document link to access the PDF document that you must complete.

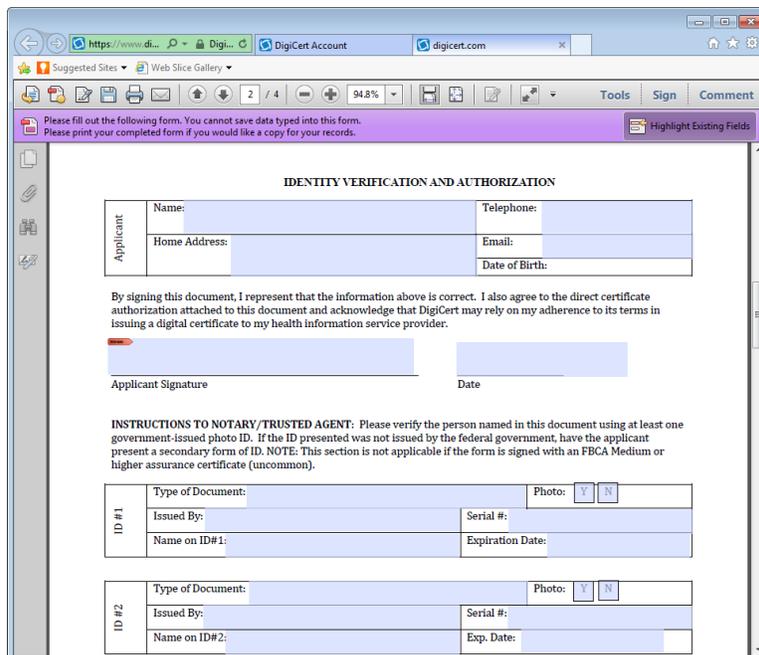


The screenshot shows a web browser window with the URL <https://www.digicert.com>. The page is titled "DigiCert Account" and contains a "Postal Code*" field with the value "75219". Below this is a "Declaration of Identity" section with the instruction: "Please download the following Declaration of Identity Document. Fill out the applicable information and sign the document. Then upload your signed declaration." A link labeled "Declaration of Identity Document (PDF)" is provided. Underneath is a "Documents" section with an "ADD DOCUMENT" button. A table with columns "Uploaded", "Name", and "Expires" is shown, but it is empty. Below the table is a "Terms of Service" section with a checkbox that is checked and labeled "I have read and agree to the terms abc". A "SAVE CHANGES" button is located at the bottom of the form.

- The Declaration of Identity Document will open in a new browser tab or window. Read the instructions on the first page, then scroll to the second page of the document.



- Complete all the information requested in the Applicant portion of the form.



- Print the document. The document will print with your completed information. You will not be able to save the form with your completed information.
- Take the printed form to a notary public. With the notary, sign and date the form. The notary can then complete their portion of the form, and notarize the document.

6. Scan the notarized document so that you have a file of the document that can be uploaded.
7. Open the email from DigiCert, and select the link to the identity verification site.
8. Scroll down, and select the Add Document button. This is located below and to the right of the Declaration of Identity Document link.
9. In the Choose File to Upload window, search for and select your scanned document file and select the Open button.
10. The date, document file name, and expiration date will be displayed in the document table.

The screenshot shows a web browser window with the URL <https://www.digicert.com>. The page contains a form for identity verification. At the top, there are input fields for 'State' (containing 'TX') and 'Postal Code*' (containing '75219'). Below these is a section titled 'Declaration of Identity' with instructions to download and sign a document. A link for 'Declaration of Identity Document (PDF)' is provided. Underneath is a 'Documents' section with an 'ADD DOCUMENT' button and a table showing one uploaded document. The table has columns for 'Uploaded', 'Name', and 'Expires'. Below the table is a 'Terms of Service' section with a checkbox for 'I have read and agree to the terms abc' and a 'SAVE CHANGES' button at the bottom.

| Uploaded | Name | Expires |
|----------------------|------------------------|----------------------|
| 31-MAR-2015 11:20 AM | Direct-Declaration.pdf | 01-MAY-2016 11:20 AM |

11. Select the I Have Read and Agree To The Terms checkbox.
12. Select the Save Changes button.
13. Close the browser window. DigiCert will process your request.

Once DigiCert has verified your identity as the authorized representative and the identity of your practice, they will issue your security certificate. When you receive the notification that the subdomain is enabled, you may begin creating direct mail addresses for your providers.