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).

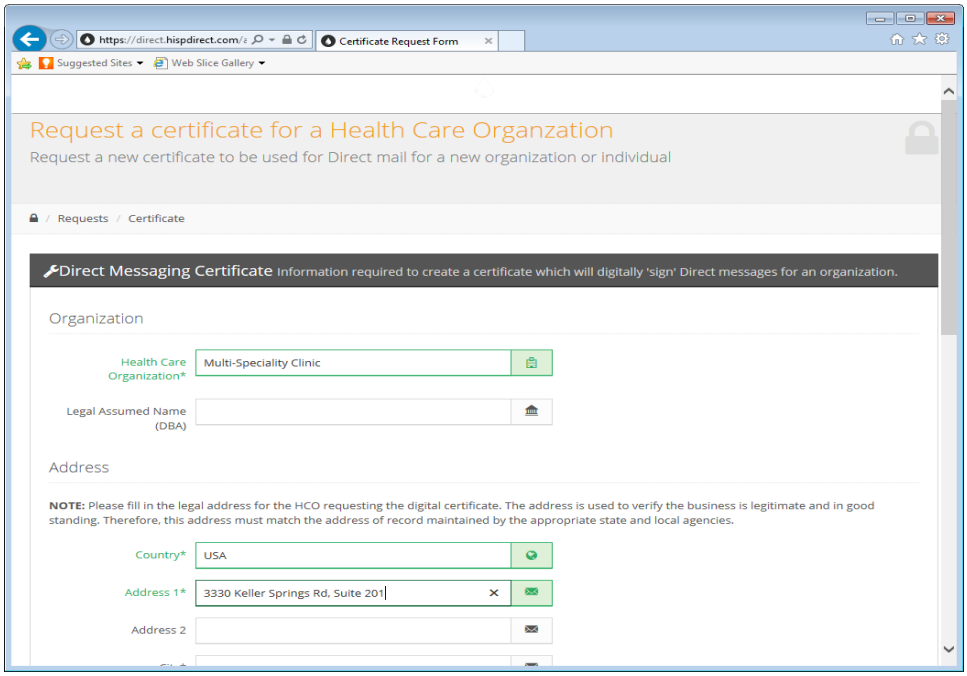
Step 1: Request DigiCert Certificate and HISPDirect Subdomain

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**.

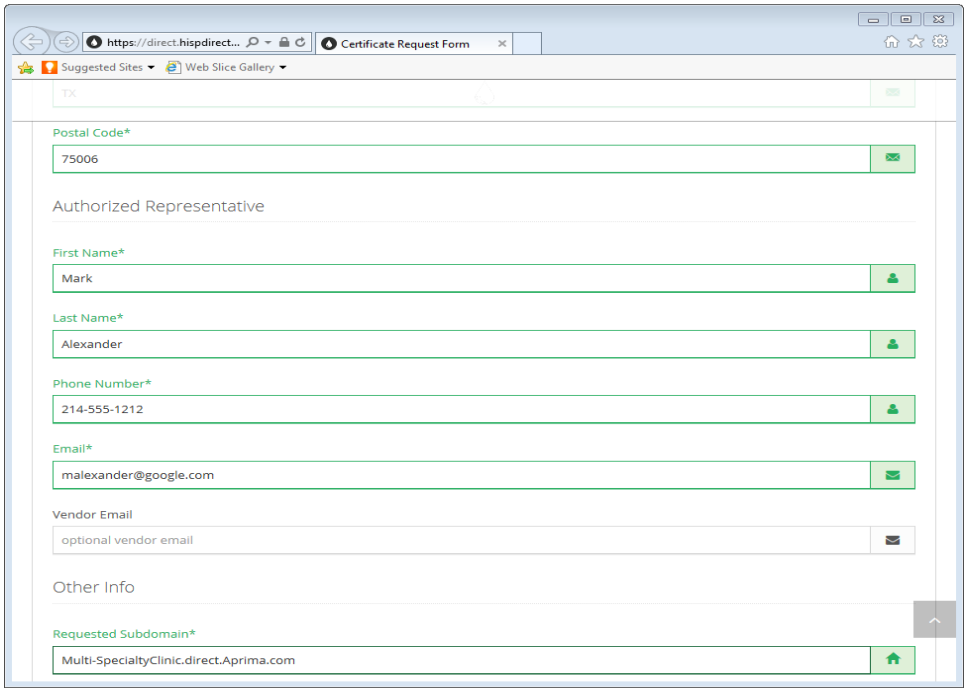


   a. In the Health Care Organization field, enter the name of the legal business entity that is your practice.

   b. If appropriate, enter a name in the Legal Assumed Name (DBA) field.

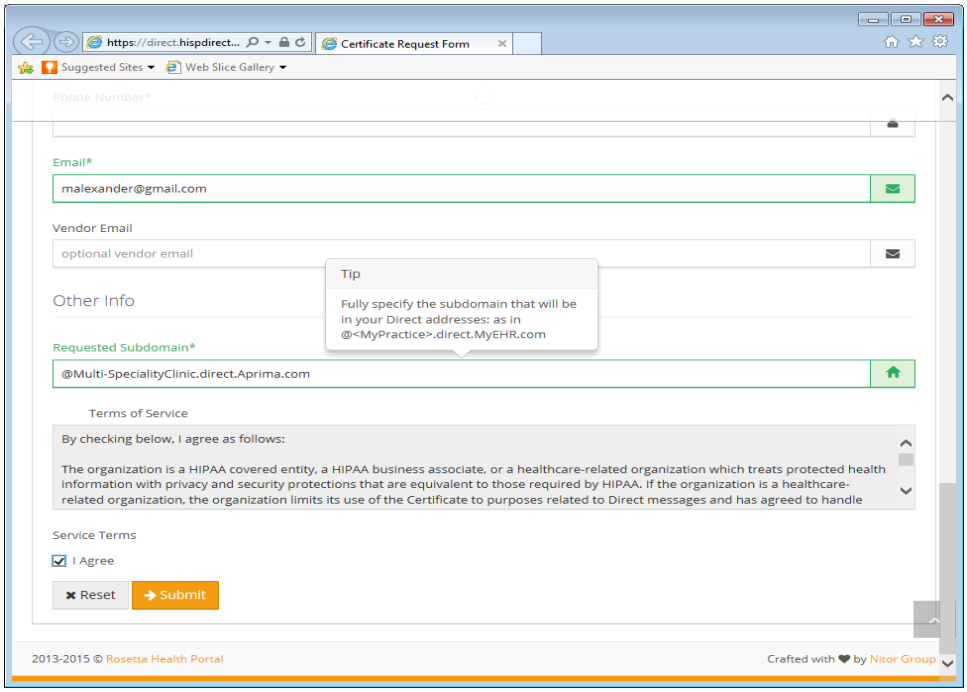
   c. In the Address section, enter the physical address of your practice. This must include the country, street address, city, state, and ZIP code.

3. Scroll down to identify your practice authorized representative.



a. Enter your First and Last Names.
b. Enter your Phone Number.
c. Enter your Email address.
d. Leave the Vendor Email address field blank.

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



   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

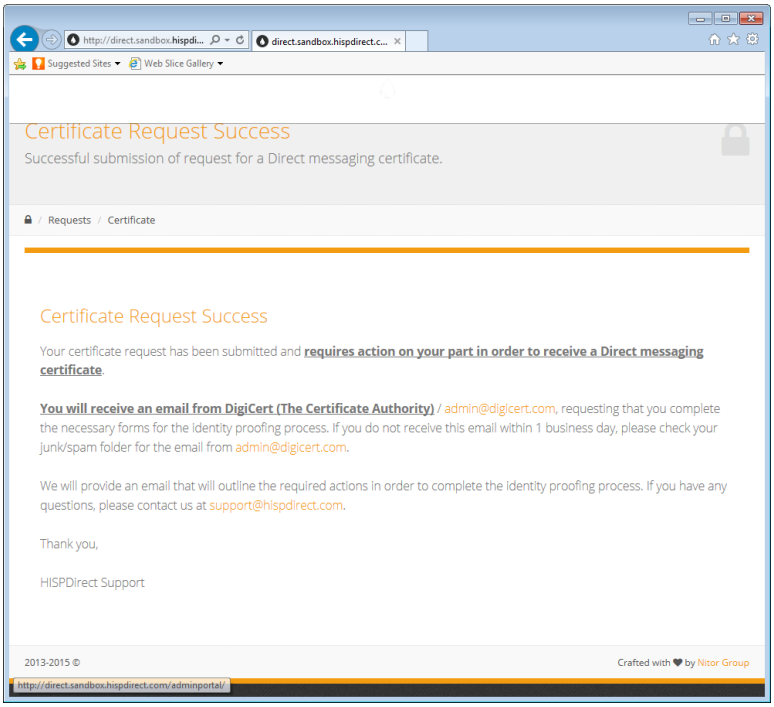
      Your practice subdomain name may include the letters (A-Z) and numbers (0-9). You may also include a hyphen (-), but the hyphen cannot be the first or the final character of the subdomain name. The subdomain cannot include any other special characters.

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 certifcate request Success message displays, close your browser window.

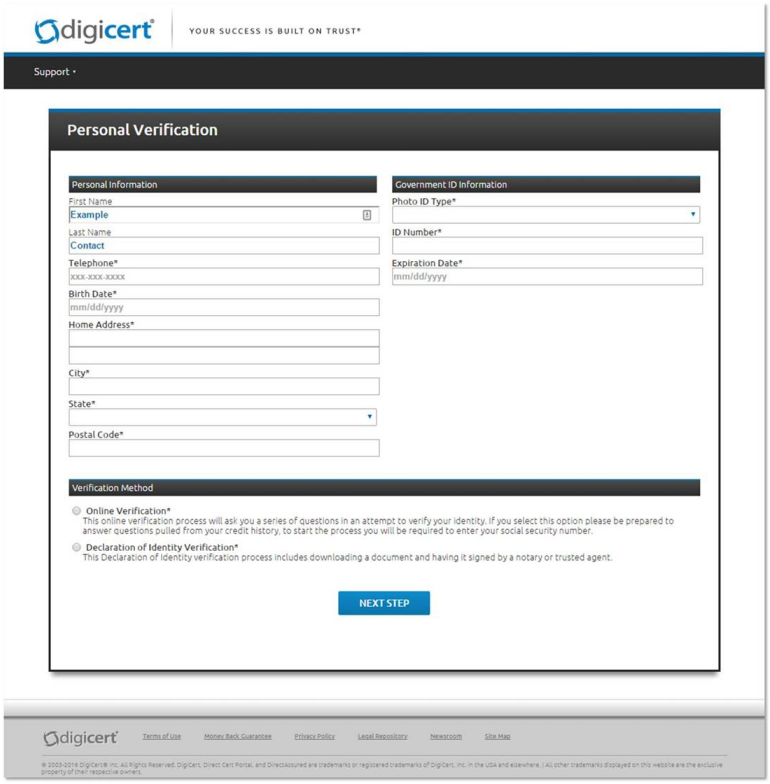


Step 2: Complete Your Identity Verification

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 propulated. Complete the rest of your personal information.



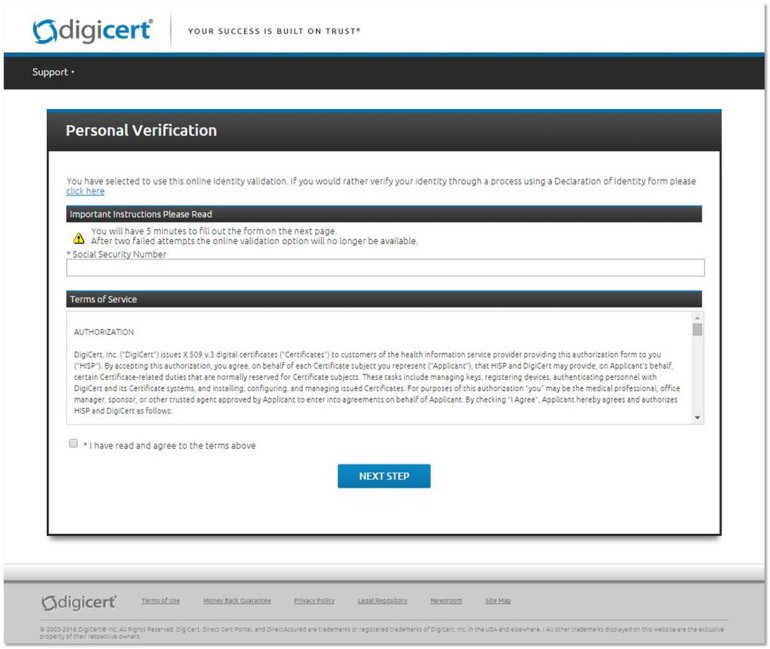
3. Scroll to the bottom, and either:
   - Select the Online Verification radio button to complete the process online. This is recommended.
   - Select the Declaration of Identity Verification rado to complete the paper verification process. This is not recommended is it can take several days (or more) 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.



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.

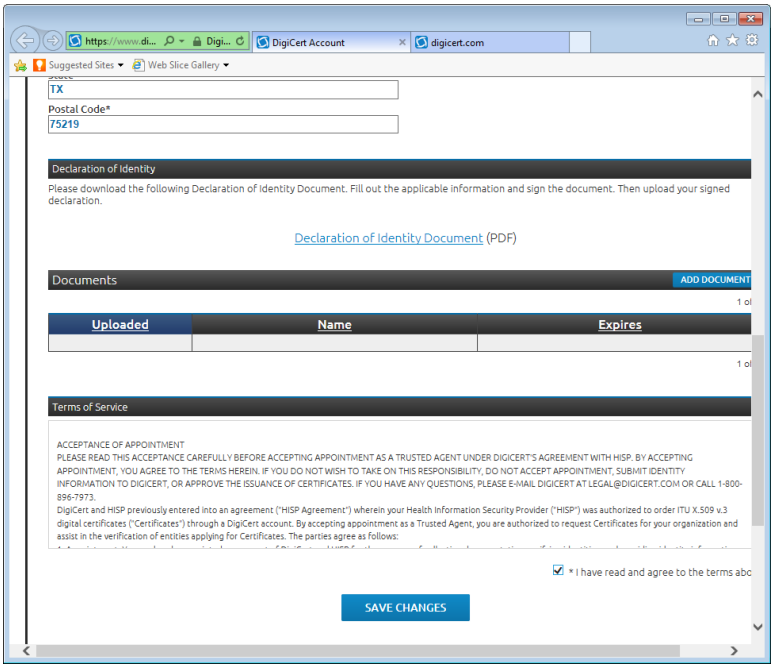
   DigiCert will then issue your security certificate to Nitor, and Nitor will enable your Direct message subdomain. When you receive notification that the subdomain is enabled, you may begin creating Direct message addresses for your providers. Instructions for creating Direct message addresses are included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

Perform the Declaration of Identity Verification Process

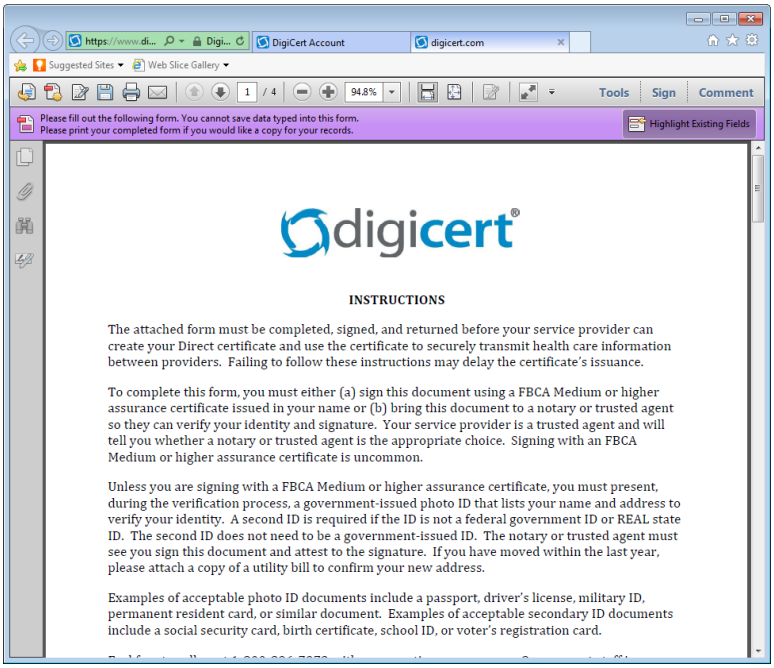
Perform this process if you selected the Declaration of Identity Verification radio button on the DigiCert Personal Verification page. In this process, you will complete, and then download and print the Declaration of Identity Document. Then, you must have the printed documented notarized. Finally, you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



2. 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.



digicert®

INSTRUCTIONS

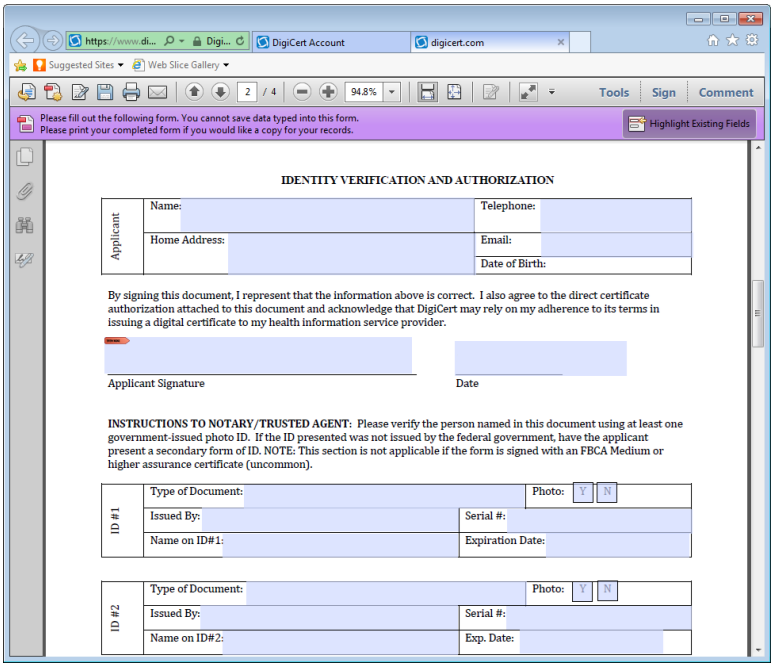
The attached form must be completed, signed, and returned before your service provider can create your Direct certificate and use the certificate to securely transmit health care information between providers. Failing to follow these instructions may delay the certificate's issuance.

To complete this form, you must either (a) sign this document using a FBCA Medium or higher assurance certificate issued in your name or (b) bring this document to a notary or trusted agent so they can verify your identity and signature. Your service provider is a trusted agent and will tell you whether a notary or trusted agent is the appropriate choice. Signing with an FBCA Medium or higher assurance certificate is uncommon.

Unless you are signing with a FBCA Medium or higher assurance certificate, you must present, during the verification process, a government-issued photo ID that lists your name and address to verify your identity. A second ID is required if the ID is not a federal government ID or REAL state ID. The second ID does not need to be a government-issued ID. The notary or trusted agent must see you sign this document and attest to the signature. If you have moved within the last year, please attach a copy of a utility bill to confirm your new address.

Examples of acceptable photo ID documents include a passport, driver's license, military ID, permanent resident card, or similar document. Examples of acceptable secondary ID documents include a social security card, birth certificate, school ID, or voter's registration card.

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



IDENTITY VERIFICATION AND AUTHORIZATION

Applicant		
	Name:	Telephone:
	Home Address:	Email:
		Date of Birth:

By signing this document, I represent that the information above is correct. I also agree to the direct certificate authorization attached to this document and acknowledge that DigiCert may rely on my adherence to its terms in issuing a digital certificate to my health information service provider.

Applicant Signature

Date

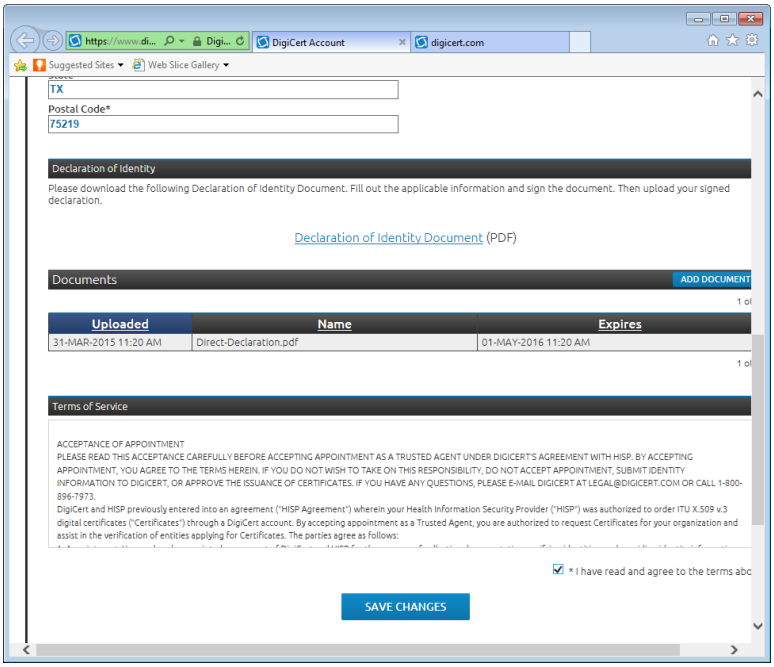
INSTRUCTIONS TO NOTARY/TRUSTED AGENT: Please verify the person named in this document using at least one government-issued photo ID. If the ID presented was not issued by the federal government, have the applicant present a secondary form of ID. NOTE: This section is not applicable if the form is signed with an FBCA Medium or higher assurance certificate (uncommon).

ID #1		
	Type of Document:	Photo: Y N
	Issued By:	Serial #:
	Name on ID#1:	Expiration Date:

ID #2		
	Type of Document:	Photo: Y N
	Issued By:	Serial #:
	Name on ID#2:	Exp. Date:

4. Print the document. The document will print with your completed information. You will not be able to save the form with your completed information.
5. 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.



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.