



Trading Partner Agreement (TPA) Request Application – User Manual

Integrated Behavioral Health Information Systems (IBHIS) Project

Los Angeles County Department of Mental Health Chief Information Office Bureau Project Management Division Integration Section

Version 1.4

1/16/2014



DOCUMENT REVISION HISTORY

Version	Release Date	Revised by	Comments/ Indicate Sections Revised
DRAFT	09/05/2013	DMH Integration Team	Draft Version of User Manual
Release Version 1.0	09/16/2013	DMH Integration Team	Release Version
Release Version 1.1	09/18/2013	DMH Integration Team	Addition of IBHIS Enrollment Section and other minor changes
Release Version 1.2	10/02/2013	DMH Integration Team	Addition of IE10 compatibility release Addition of instructions under Digital Key – Assignment Process
Release Version 1.3	10/28/2013	DMH Integration Team	B.1. Changed location of TPA Request Application Link under EDI Certification. C.2. Addition of “Provider Connect” in EDI transaction list for Network Providers. - Modified fields (Required / Optional) - Modified Layout - Updated screen shots D.2. Added next steps
Release Version 1.4	1/16/2014	DMH Integration Team	C.2. Addition of Notes in steps 1 and 2 of auto e-mail notification to Trading Partner D.2. Addition of Exporting “Private Key” instructions Updated screenshots and other minor changes



Table of Contents

A.	INTRODUCTION.....	3
A.1.	Purpose.....	3
A.2.	Overview.....	3
B.	IBHIS ENROLLMENT.....	3
B.1.	Accessing the TPA Request Application.....	4
C.	TPA PROCESS.....	7
C.1.	Login into the TPA Request Application.....	7
C.2.	Create Request.....	11
C.3.	Save/Draft Request.....	16
C.4.	Edit Request.....	17
C.5.	Submit Request.....	18
C.6.	View Status of a Request.....	19
D.	DIGITAL KEY – ASSIGNMENT PROCESS.....	23
D.1	Install the Key.....	23
D.2	Additional Instructions (Key Set Up).....	30



A. INTRODUCTION

A.1. Purpose

The purpose of this application is to manage the process of electronically collecting Trading Partner Agreement (TPA) forms, and pertinent information, from Legal Entities and Network Providers who will be exchanging information with the Department of Mental Health (DMH) via Electronic Data Interchange (EDI) for the Integrated Behavioral Health Information System (IBHIS). Those with a current TPA for electronic data exchange with the Integrated System (IS) and those who have never completed a TPA for data exchange with the IS must complete a TPA to initiate the credentialing process for electronic data exchange with the IBHIS.

A.2. Overview

The following are many benefits to the use of this application:

- With this “electronic” process, you will not submit paper forms.
- Contract Providers (CPs) will be able to download, sign, scan and upload their TPAs.
- CPs will be notified via emails regarding the submission and approval of their respective TPAs.
- Instead of calling the Helpdesk, CPs will be able to view their status throughout the credentialing process.
- DMH staff members will be able to track the credentialing process status of all CPs.

B. IBHIS ENROLLMENT

The purpose of Integrated Behavioral Health Information System (IBHIS) Enrollment is so that Trading Partners can start the IBHIS Electronic Data Interchange (EDI) Process with the Department of Mental Health (DMH).

The Legal Entity and Network providers must submit and receive transactions for claiming services in accordance with their DMH Agreement. For EDI, providers are required to exchange transactions via an Electronic File Transfer (EFT) method. The requirements for this method are included in the **Trading Partner Agreement (TPA)**.

To enroll in the EDI process, Legal Entity and Network providers must complete a TPA request online.

B.1. Accessing the TPA Request Application

1. Access the **IBHIS Website** by clicking or typing the following URL in your browser:

<http://lacdmh.lacounty.gov/hipaa/index.html>

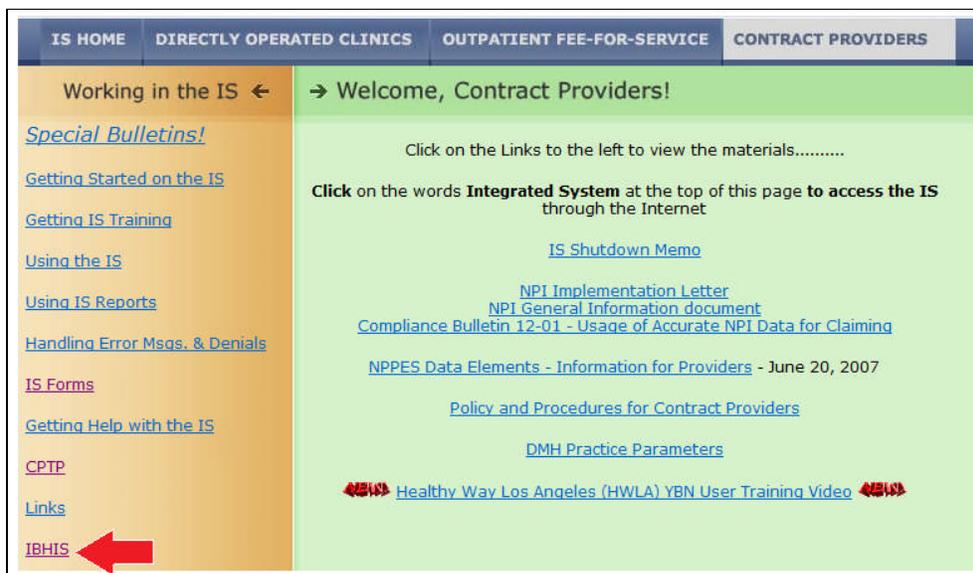
2. From the home page, choose one of the following appropriate actions:

For Legal Entity providers:

1) Click the **Contract Providers** tab.



2) Click the **IBHIS** link.



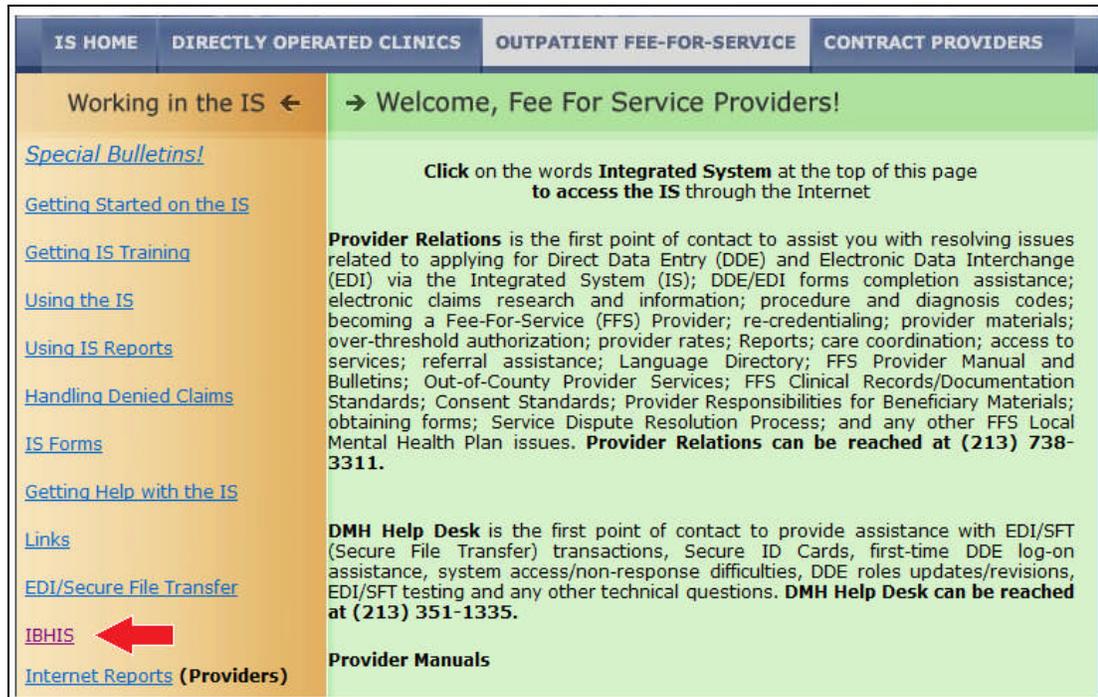


For Network providers:

- 1) Click the **Outpatient-Fee-For Service** tab.



- 2) Click the **IBHIS** link.



For Legal Entity and Network providers:

1. From the IBHIS page, click the **IBHIS EDI Certification** link.



2. Click the **TPA Application Link**.





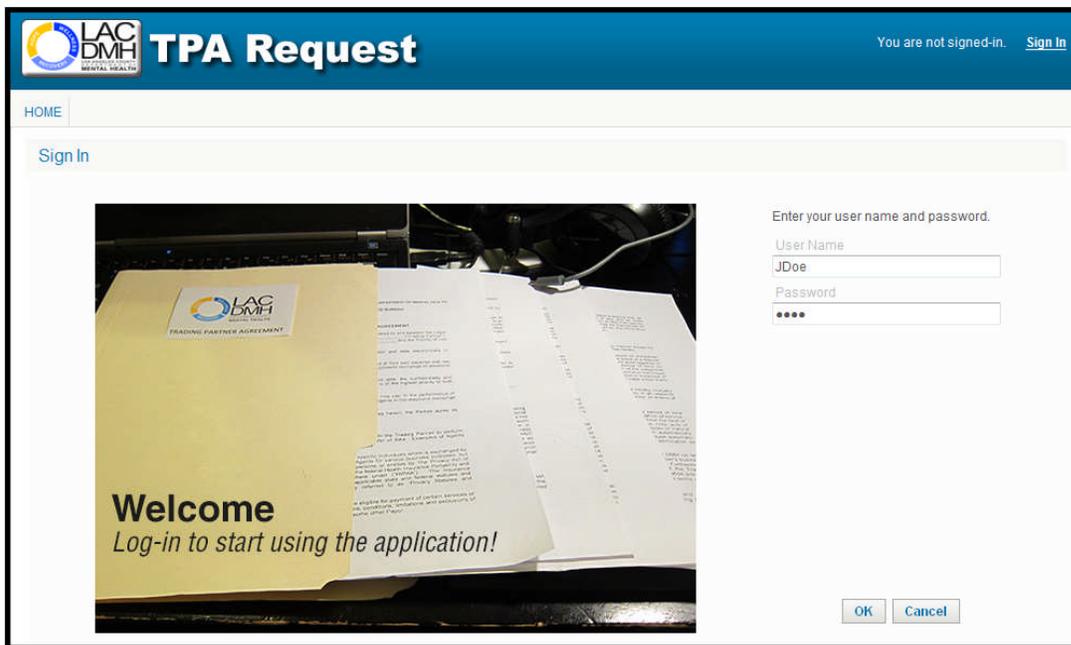
C. TPA PROCESS

NOTE: This system is designed for Internet Explorer browser (VERSIONS 7, 8, 9 and 10). Users experience may vary with other browsers (e.g. Safari, FIREFOX, CHROME, etc.)

C.1. Login into the TPA Request Application

1. Log into the application by entering your **User Name** and **Password**.
2. Click **OK**, or hit Enter.

NOTE: The user name and password is the same used to login to the Integrated System (IS). If you do not know your IS User Name and Password, please contact the DMH helpdesk to reset it at (213) 351-1335.



Note: Only one (1) TPA Request may be submitted per Trading Partner.

Once you are logged in:

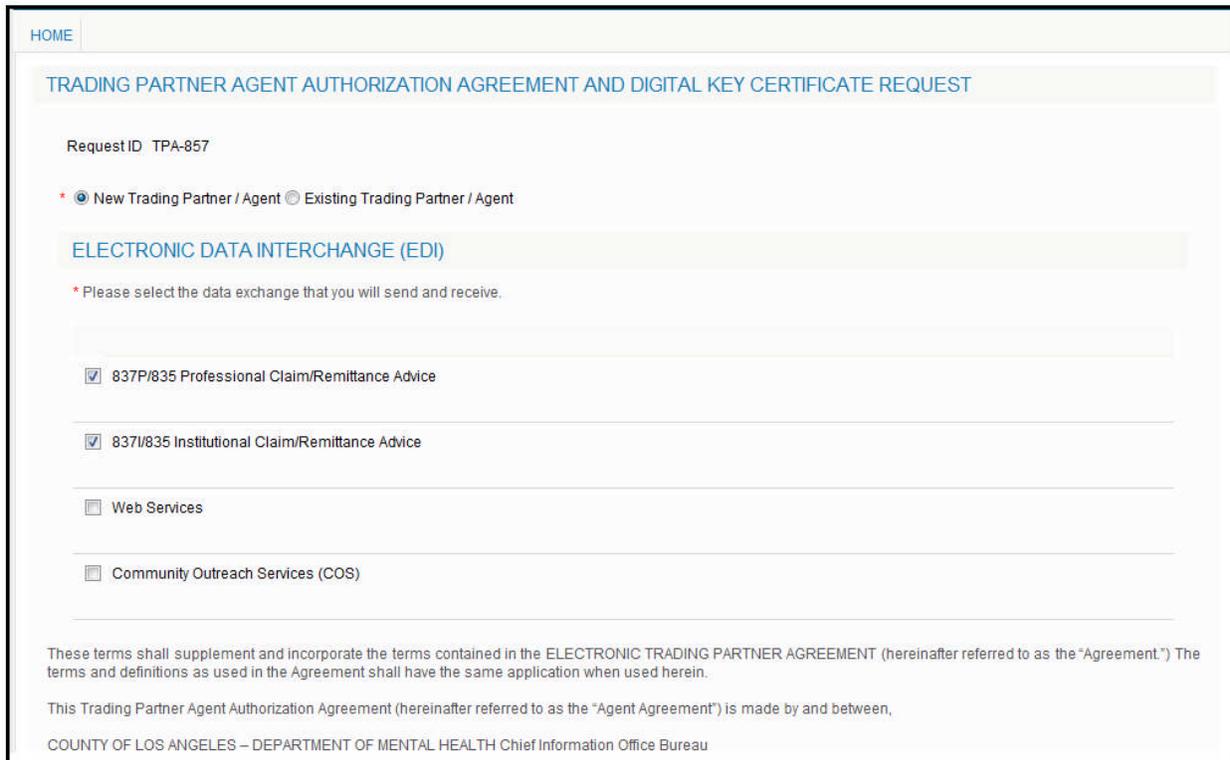
Step 1- For a Legal Entity and Network Providers (associated to one (1) provider): The **TPA Request Status** page will be displayed.

Note: For Network Providers associated to multiple providers, skip to Step 1a.

- To start the TPA request, click the  Edit Icon.

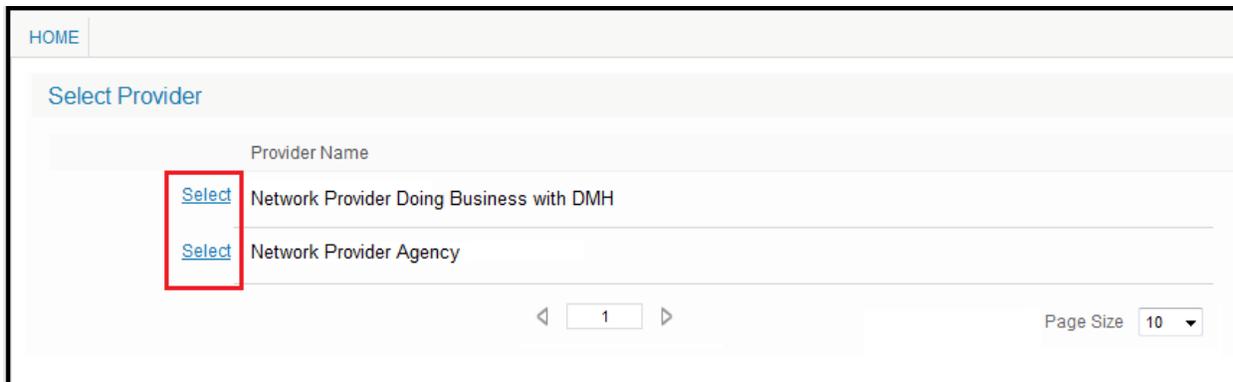


- The TPA Request form will be displayed.

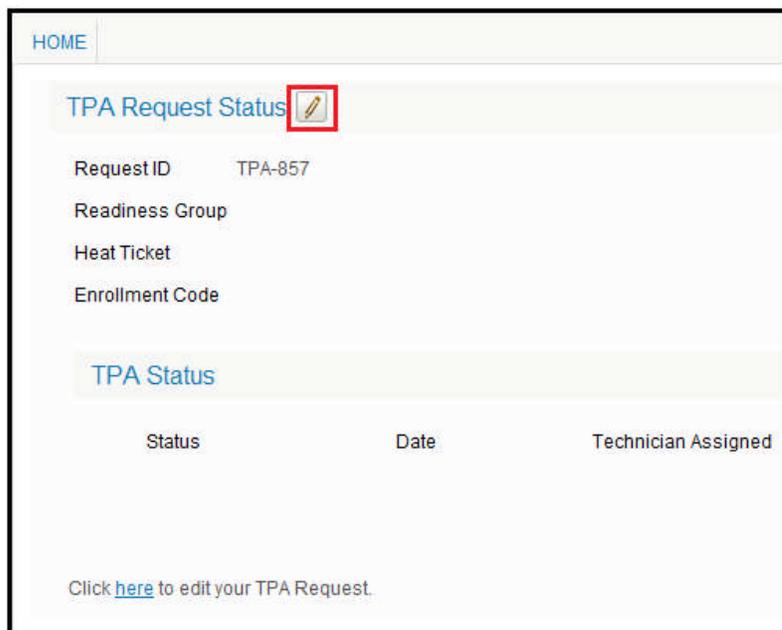


Note: Legal Entity and Network Providers associated to one (1) provider, skip to Section C2.

Step 1a- For Network Providers (with multiple providers): The **Select Provider** page will be displayed. You will have the option to select the provider you wish to create the TPA request for.



- To start the TPA request, click the  Edit Icon.





- The **TPA Request** form will be displayed.

HOME

TRADING PARTNER AGENT AUTHORIZATION AGREEMENT AND DIGITAL KEY CERTIFICATE REQUEST

Request ID TPA-857

* New Trading Partner / Agent Existing Trading Partner / Agent

ELECTRONIC DATA INTERCHANGE (EDI)

* Please select the data exchange that you will send and receive.

837P/835 Professional Claim/Remittance Advice

837I/835 Institutional Claim/Remittance Advice

Web Services

Community Outreach Services (COS)

These terms shall supplement and incorporate the terms contained in the ELECTRONIC TRADING PARTNER AGREEMENT (hereinafter referred to as the "Agreement.") The terms and definitions as used in the Agreement shall have the same application when used herein.

This Trading Partner Agent Authorization Agreement (hereinafter referred to as the "Agent Agreement") is made by and between,

COUNTY OF LOS ANGELES – DEPARTMENT OF MENTAL HEALTH Chief Information Office Bureau

C.2. Create Request

Step 1- Fill out the TPA Form:

1. Select whether you are a New Trading Partner / Agent or an Existing Trading Partner / Agent.

TRADING PARTNER AGENT AUTHORIZATION AGREEMENT

Request ID TPA-857

* New Trading Partner / Agent Existing Trading Partner / Agent

Electronic Data Interchange (EDI)

2. Select the data interchange (interfaces) that applies to you (more than one may be selected).

Note: Network Providers will have a “Provider Connect” option.

Legal Entity Options:	Network Provider Options:
<p style="color: #0070C0; font-weight: bold;">ELECTRONIC DATA INTERCHANGE (EDI)</p> <p>* Please select the data exchange that you will send and receive.</p> <p><input checked="" type="checkbox"/> 837P/835 Professional Claim/Remittance Advice</p> <p><input checked="" type="checkbox"/> 837I/835 Institutional Claim/Remittance Advice</p> <p><input type="checkbox"/> Web Services</p> <p><input type="checkbox"/> Community Outreach Services (COS)</p>	<p style="color: #0070C0; font-weight: bold;">ELECTRONIC DATA INTERCHANGE (EDI)</p> <p>* Please select the data exchange that you will send and receive.</p> <p><input type="checkbox"/> 837P/835 Professional Claim/Remittance Advice</p> <p><input type="checkbox"/> 837I/835 Institutional Claim/Remittance Advice</p> <p><input type="checkbox"/> Web Services</p> <p><input type="checkbox"/> Community Outreach Services (COS)</p> <div style="border: 1px solid red; padding: 2px; display: inline-block;"> <p><input checked="" type="checkbox"/> Provider Connect</p> </div>



Trading Partner Information (* indicates information is required)

3. **Trading Partner Type:** The agency’s type (Legal Entity or Network Provider) is a **required** and pre-populated field.
4. **Legal Entity / Network Provider Name:** The Legal Entity or Network Provider name is a **required** and pre-populated field. Verify that the information is correct.
5. **Legal Entity / Network Provider Number:** The Legal Entity or Network Provider number is a **required** and pre-populated field. Verify that the information is correct.
6. **Payee NPI Number:** The agency’s Payee National Provider Identifier (NPI) is a 10-digit number **required** field.
7. **DUNS Number:** The agency’s Data universal Number System (DUNS) is a 9-digit number **required** field.
8. **Authorized Contact Name:** The name of the individual that is authorized to sign the Trading Partner Agreement is a **required** field.
9. **Authorized Contact Title:** The title of the individual that is authorized to sign the Trading Partner Agreement is a **required** field.
10. **Address:** The agency’s address is a **required** field.
11. **State:** The agency’s State is a **required** field
12. **City:** The agency’s City is a **required** field.
13. **Zip:** The agency’s Zip is a **required** field.
14. **Telephone:** The Telephone of the individual who is authorized to sign the Trading Partner Agreement is a **required** field. Follow this telephone number format: 9999999999.
15. **Fax Number:** The Authorized Contact’s Fax Number field is optional.
16. **Email Address:** The Authorized Contact’s e-mail address field is optional.
Note: A notification will be sent to this email address when a test and/or production key are sent to the IT Contact.

TRADING PARTNER INFORMATION

* indicates field is required.

* Trading Partner Type	Legal Entity		
* Legal Entity Name	<input type="text" value="Legal Entity Doing Business with DMH"/>		
* Legal Entity Number	<input type="text" value="00999"/>		
* Payee NPI Number	<input type="text" value="9999999999"/>		
* DUNS Number	<input type="text" value="999999999"/>		
* Authorized Contact Name	<input type="text" value="John Doe"/>		
* Authorized Contact Title	<input type="text" value="CEO"/>		
* Address	<input type="text" value="1234 S. Lane Street"/>		
* City	<input type="text" value="Los Angeles"/>	* State	<input type="text" value="California"/>
* Telephone	<input type="text" value="9999999999"/>	* ZIP	<input type="text" value="90099"/>
Fax Number	<input type="text"/>		
Email Address	<input type="text" value="JDoe@gmail.com"/>		



Trading Partner Digital Certificate / Technical / EDI Contact Information (* indicates information is required)

This is the section where you can submit information of a technical resource that will be helping with Digital Key download and/or submitting EDI files of your agency to DMH.

1. **Name:** The name of the individual that will be installing the IBHIS Digital Key is a **required** field.
2. **Title:** The title of the individual that will be installing the IBHIS Digital Key field is optional.
3. **Address:** The address of the individual that will be installing the IBHIS Digital Key field is optional.
4. **State:** The State of the individual that will be installing the IBHIS Digital Key field is optional.
5. **City:** The City of the individual that will be installing the IBHIS Digital Key field is optional.
6. **Zip:** The Zip of the individual that will be installing the IBHIS Digital Key field is optional.
7. **Telephone:** The Telephone of the individual who will be installing the IBHIS Digital Key is a **required** field. The telephone number format is: 9999999999.
8. **Email Address:** The e-mail of the individual who is responsible for downloading the IBHIS Digital Key in your organization is a **required** field.

Note: The e-mail in this section will be used when setting-up the user account in MPKI system, in order to receive Test and Production Digital Keys. Instructions on how to install the keys will be sent to this email address.

TRADING PARTNER DIGITAL CERTIFICATE / TECHNICAL / EDI CONTACT INFORMATION

Please make sure that this information pertains to the individual that will be installing the Digital Certificate. The e-mail with instructions to install the certificate will be sent to this email address.

* Name

Title

Address

City State ZIP

* Telephone

Fax Number

*Email Address



Step 2- Of the following; provide the information that is applicable to your request:

Billor Information, Clearinghouse Information, Software Vendor Information, and/or Consultant Information.

Note: Email addresses provided in any of the following sections, will receive an email notification, once the test and production keys are sent to the IT Contact.

- Click  to expand or collapse each section.

 **BILLER INFORMATION**

Organization Name

Authorized Contact Name

Authorized Contact Title

Address

City State ZIP

Telephone

Fax Number

Email Address

IF CLEARINGHOUSE WILL BE USED FOR DATA INTERCHANGE, PLEASE COMPLETE THE FOLLOWING FIELDS:

 **CLEARINGHOUSE INFORMATION**

IF SOFTWARE VENDOR WILL BE USED FOR DATA INTERCHANGE, PLEASE COMPLETE THE FOLLOWING FIELDS:

 **SOFTWARE VENDOR INFORMATION**

IF CONSULTANT WILL BE USED FOR DATA INTERCHANGE, PLEASE COMPLETE THE FOLLOWING FIELDS:

 **CONSULTANT INFORMATION**



Trading Partner Business Contact: This is the section where you can submit contact information of a person who is an expert in business operations at your agency.

Note: Email address provided in this section, will receive an email notification, once the test and production keys are sent to the IT Contact.

TRADING PARTNER BUSINESS CONTACT INFORMATION

Name

Title

Address

City State ZIP

Telephone

Fax Number

Email Address

Step 3- The signed TPA must be attached for the request to be processed. Follow the steps described below to download, print, sign, scan, and upload the original TPA form with your TPA request.

1. Click the word **here** to download the blank Trading Partner Agreement.
2. Print it, sign it, scan and save it to your PC in a convenient location.

NOTE: The person signing must have contract signing authority.

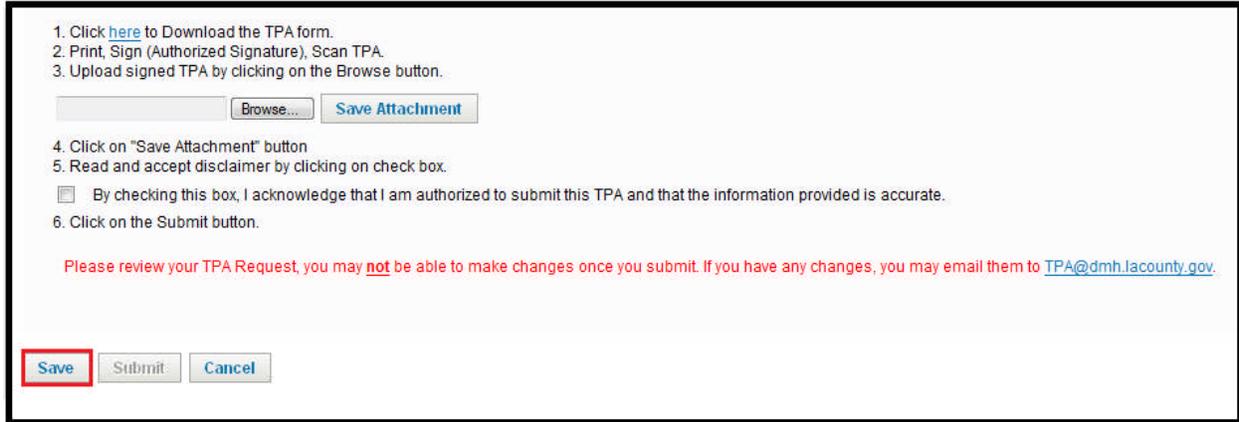
3. Click the **Browse** button to find the TPA document which you have saved in the step above, and select it.

NOTE: You may **ONLY** save these file formats: PDF, JPG, PNG, BMP and/or Jpeg.

4. Click the **Save Attachment** button. You will get a confirmation notification that your file has been uploaded.
5. Click the check box to acknowledge that you have authority to submit the TPA and that all information is accurate.

C.3. Save/Draft Request

The TPA form may be saved until it is ready to be submitted by clicking the “**Save**” button.



1. Click [here](#) to Download the TPA form.
2. Print, Sign (Authorized Signature), Scan TPA.
3. Upload signed TPA by clicking on the Browse button.

4. Click on "Save Attachment" button
5. Read and accept disclaimer by clicking on check box.
 By checking this box, I acknowledge that I am authorized to submit this TPA and that the information provided is accurate.
6. Click on the Submit button.

Please review your TPA Request, you may **not** be able to make changes once you submit. If you have any changes, you may email them to TPA@dmh.lacounty.gov.

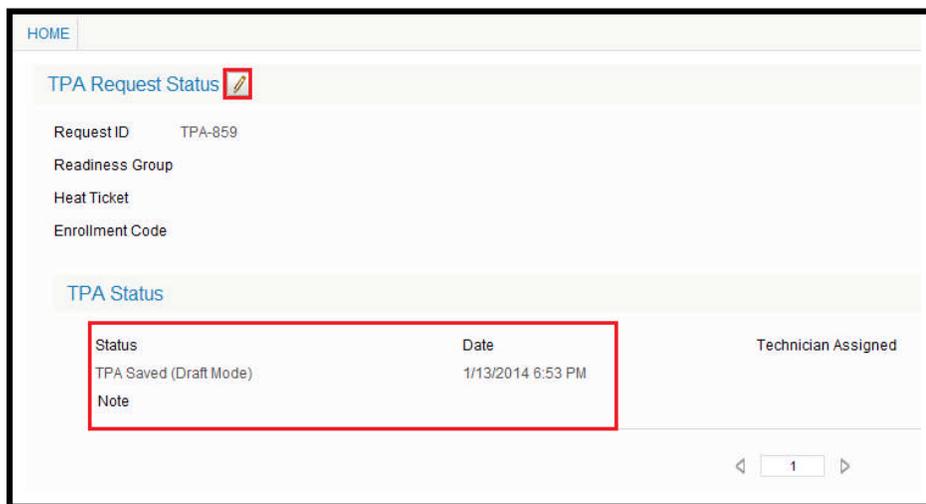
- Once the form has been saved, click the **Home** tab to be routed to the **TPA Status** page to view the status of your request and to continue filling out the request.

Note: The next time you login to the system, you will be routed to **TPA Status** page.

C.4. Edit Request

While on Draft Mode, the edit icon will continue to be enabled, and the **TPA Status** will display “TPA Saved (Draft Mode)”.

To edit a TPA Request form while on Draft Mode, click the  icon. Make any necessary changes before submission.



Note: Only one (1) TPA Request may be submitted per Trading Partner. Once the form has been submitted, during this process **you may NOT edit the information**. If you need to modify a TPA, you will need to e-mail changes to: TPA@dmh.lacounty.gov. You will receive confirmation when the change has been made.



C.5. Submit Request

Step 1- To submit the TPA Request form, complete the required information, ensure that the signed original TPA form is attached and the acknowledgment checkbox is selected.

- Once the acknowledgment checkbox is selected, the **Submit** button will be enabled.
- Click **Submit**.

1. Click [here](#) to Download the TPA form.
2. Print, Sign (Authorized Signature), Scan TPA.
3. Upload signed TPA by clicking on the Browse button.

Your attachment was successfully uploaded.

4. Click on "Save Attachment" button
5. Read and accept disclaimer by clicking on check box.
 By checking this box, I acknowledge that I am authorized to submit this TPA and that the information provided is accurate.
6. Click on the Submit button.

Please review your TPA Request, you may **not** be able to make changes once you submit. If you have any changes, you may email them to TPA@dmh.lacounty.gov.

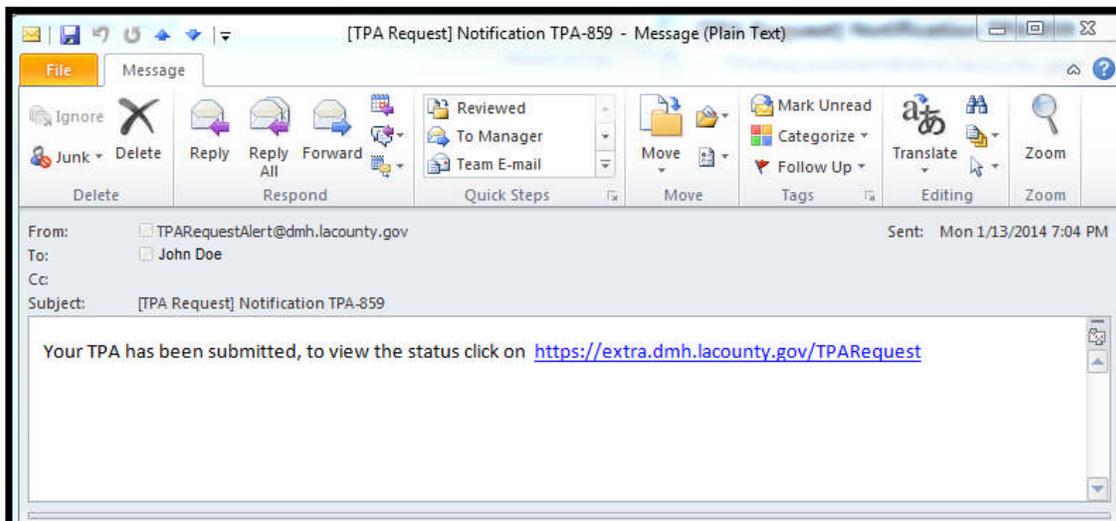
Step 2- Once the TPA form has been submitted, a confirmation page and TPA Request confirmation number will be displayed. Click the **OK** button to be routed to the TPA Status Page.

HOME

Trading Partner Agreement Sent

Your TPA Request ID is TPA-859. Please click OK to return HOME.

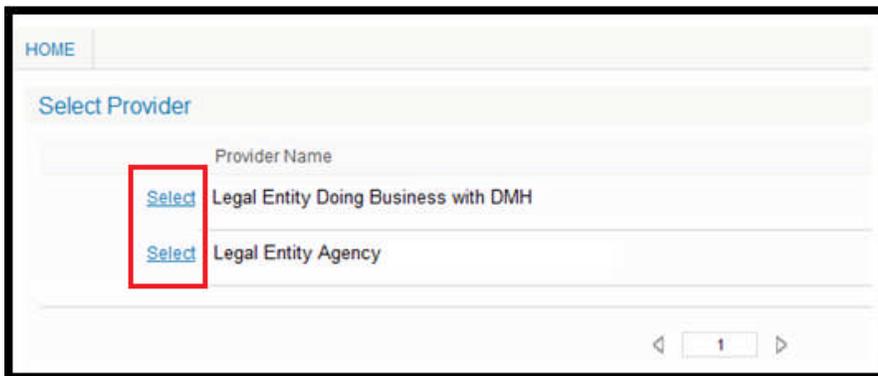
- After the TPA Request has been submitted an email notification will be sent to the individual submitting the TPA.



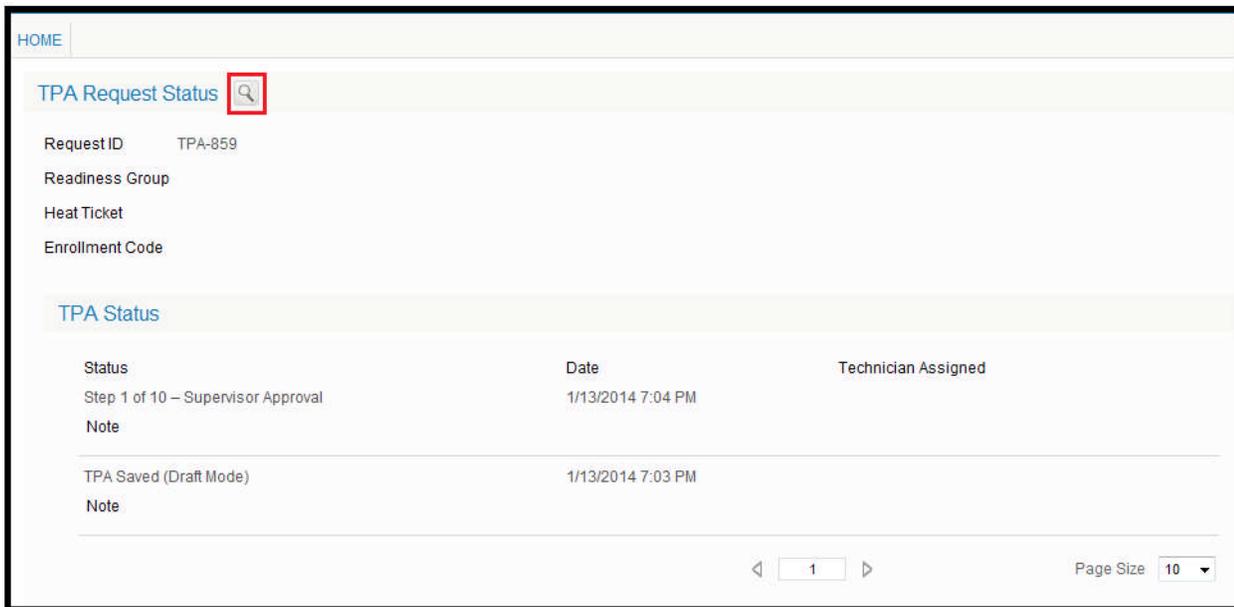
C.6. View Status of a Request

Step 1- To view the TPA status for a provider; select the provider you wish to see the status for.

Note: If you are only associated to one provider, skip to Step 2.



Step 2- The **TPA Request Status** page will display the status of the request.



HOME

TPA Request Status 

Request ID TPA-859

Readiness Group

Heat Ticket

Enrollment Code

TPA Status

Status	Date	Technician Assigned
Step 1 of 10 – Supervisor Approval	1/13/2014 7:04 PM	
TPA Saved (Draft Mode)	1/13/2014 7:03 PM	

Note

Note

Page Size 10

Step 3- Click the  Show icon to view the completed TPA Request form.

Once your TPA is approved, a technician will be assigned to process this request. You may log in to the application to see the status at any time.



The following are the descriptions of the steps:

TPA Saved (Draft Mode): This status will be shown when you click on the **Save** button.

Step 1 of 10 – Supervisor Approval: After reviewing the TPA request and validating the signatures of the authorized party in the attached agreement, this status shows that the request was approved by the DMH Administrator.

Step 2 of 10 – Technician Assigned: This status reflects that a Provisioning Technician has been assigned to work on your request.

Step 3 of 10 – Enrollment Code Added: This status indicates that after validating and setting up your profile to receive a Test Digital Key, a unique Code has been added to your TPA request. In order for you to download the Test Digital Key, you will be prompted to enter your Enrollment Code.

Step 4 of 10 – Test Keys sent to TP: This status specifies that the link to download your Test Digital Key has been sent to your email address.

Step 5 of 10 – Completed Digital Key Testing: Using your newly installed Test Digital Key, you will be instructed to connect to the IBHIS file drop-off location to drop sample test file(s) to test the digital key. This status is to confirm that DMH has established successful communications with your agency.

Step 6 of 10 – Structural Validation Status: This status indicates whether these sample EDI test files, or Community Outreach Services (COS) sample flat file(s), conform(s) to structural rules.

Step 7 of 10 – HIPAA (EDI Only) Validation Status: This status reflects whether these sample EDI test files conform to HIPAA rules.

Step 8 of 10 – Business Rule Validation Status: This status indicates that the Test files have passed the structural validation and are ready for IBHIS Business Rules validation.

Step 9 of 10 – Ready for Production: This status will let the Provisioning Technician know that the Test file(s) have successfully passed the IBHIS Business Rules.

Step 10 of 10 – Production Key Packet Set: Similar to the link you would have received in Step 4 of 10, this status indicates that DMH has sent you a link to install the Production Digital Key for your Production environment. A **new enrollment code** will replace the code entered previously for testing purposes.

Modified TPA: This status is to track TPA's that have been modified by the Administrator or Provisioning Technician if requested by the Trading Partner.

Contact Technician - The purpose of this status is for the technician(s) to reach out and ask the user to call them, (if the technician has no success reaching the user). The reason and contact information should be indicated in the note section.

Additional Comments - The purpose of this status is for a technician to add additional comments outside of the 10 steps.

*****IMPORTANT*****

The next step will be to install a test certificate on your computer.

Within a week you will receive an e-mail from:

Enterprise PKI Support <support@pki.symantec.com>

Once you receive the e-mail, follow the next steps.

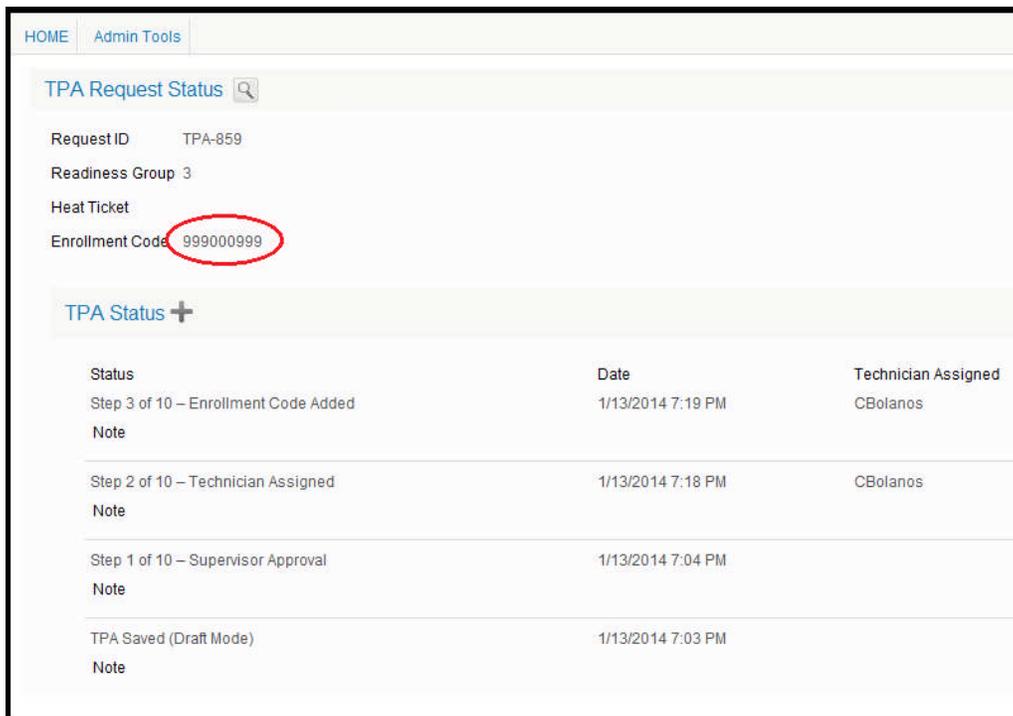
D. DIGITAL KEY – ASSIGNMENT PROCESS

D.1 Install the Key

Please follow the following steps to successfully install the Key.

Step 1: You will get an email from the Symantec system. There will be two steps to follow.

First, get your certificate enrollment code from your **TPA Request Application** status section.



The screenshot shows the 'TPA Request Status' page. At the top, there are navigation links for 'HOME' and 'Admin Tools'. Below that is a search bar for 'TPA Request Status'. The main content area displays the following information:

- Request ID: TPA-859
- Readiness Group: 3
- Heat Ticket:
- Enrollment Code: 999000999 (circled in red)

Below this information is a section titled 'TPA Status +' which contains a table of status updates:

Status	Date	Technician Assigned
Step 3 of 10 – Enrollment Code Added Note	1/13/2014 7:19 PM	CBolanos
Step 2 of 10 – Technician Assigned Note	1/13/2014 7:18 PM	CBolanos
Step 1 of 10 – Supervisor Approval Note	1/13/2014 7:04 PM	
TPA Saved (Draft Mode) Note	1/13/2014 7:03 PM	

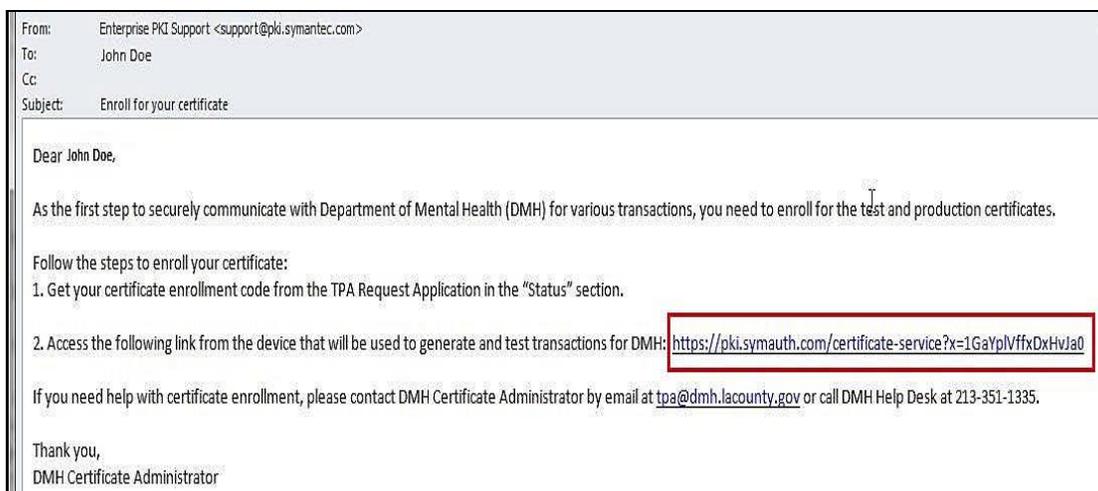
Second, log onto the computer you will be using to generate/test transactions for DMH.

- Click the link and open it up in Internet Explorer.

STOP!!!

Before installing certificate, Internet Explorer browser is recommended as we do not support other versions or browsers (e.g. Safari, FIREFOX, CHROME, etc.).

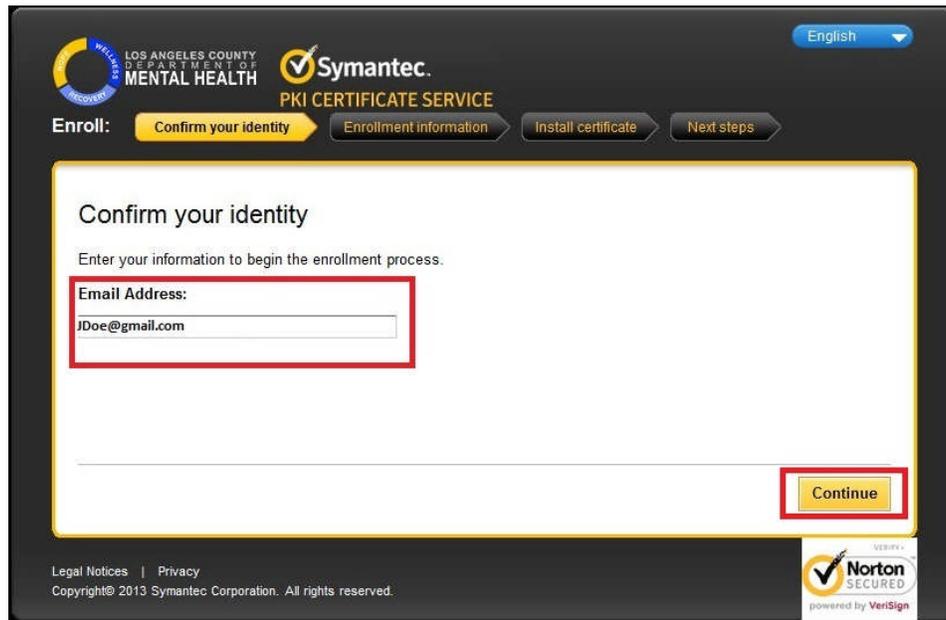
In order to successfully download DMH Digital Key, your computer must have Active-X plug-in installed. An administrator from your organization can help with setting up the Active-X plug-in for your machine.



- The Symantec's digital certificate **Enroll** page will be displayed.

Step 2: To confirm your identity – enter your email address in the **Email Address** field. This should be the same email you provided DMH in the TPA Request Form.

- Click **Continue**.



English

LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH

Symantec.
PKI CERTIFICATE SERVICE

Enroll: **Confirm your identity** Enrollment information Install certificate Next steps

Confirm your identity

Enter your information to begin the enrollment process.

Email Address:
JDoe@gmail.com

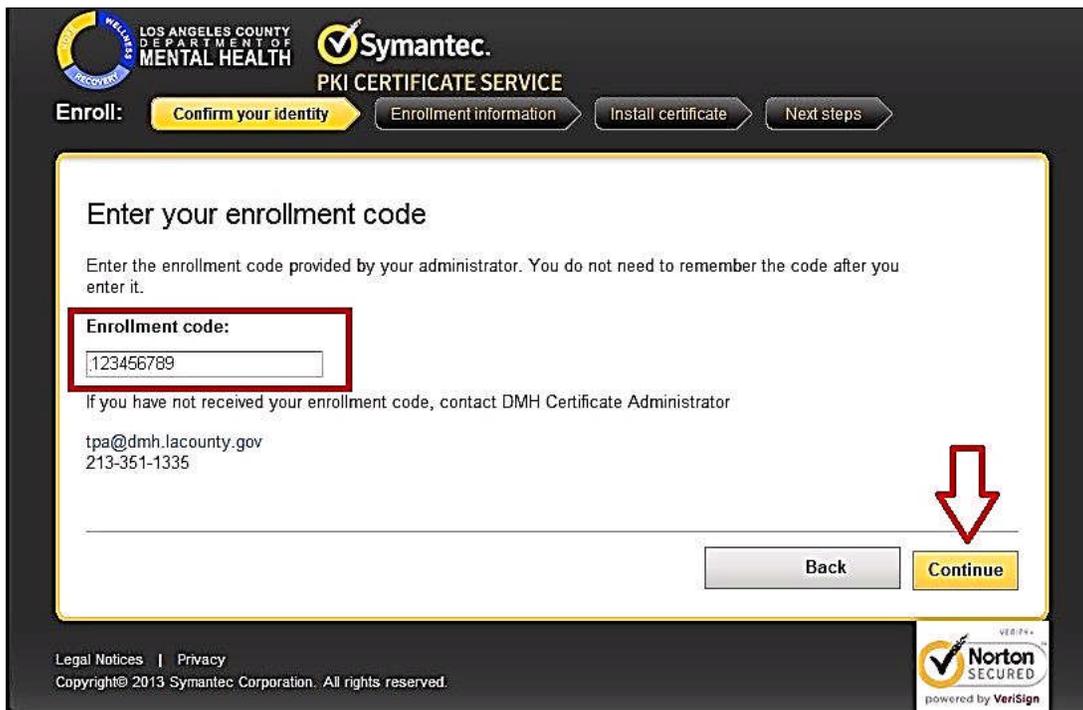
Continue

Legal Notices | Privacy
Copyright © 2013 Symantec Corporation. All rights reserved.

Norton
SECURED
powered by VeriSign

Step 3: Enter the enrollment code you received from the TPA Request Application Status page in the **Enrollment code** box.

- Click **Continue**.



LOS ANGELES COUNTY DEPARTMENT OF MENTAL HEALTH

Symantec.
PKI CERTIFICATE SERVICE

Enroll: **Confirm your identity** | Enrollment information | Install certificate | Next steps

Enter your enrollment code

Enter the enrollment code provided by your administrator. You do not need to remember the code after you enter it.

Enrollment code:

If you have not received your enrollment code, contact DMH Certificate Administrator

tpa@dmh.lacounty.gov
213-351-1335

Back **Continue**

Legal Notices | Privacy
Copyright © 2013 Symantec Corporation. All rights reserved.

Norton SECURED
powered by VeriSign



Step 4: You'll get a message showing **Identity confirmed**. Verify all the information. If anything needs to be corrected, contact LA County's DMH Certificate Administrator at TPA@dmh.lacounty.gov. Otherwise, click **Continue**.

Enroll: Confirm your identity | **Enrollment information** | Install certificate | Next steps

Identity confirmed.

Verify your information

Verify that the information associated with your certificate is correct, and complete any required fields.

Other Name (UPN)	JDoe
First name	John
Last name	Doe
Organizational Unit (OU)	Legal Entity Doing Business with DMH
Organization	Legal Entity Doing Business with DMH
Locality	LA
State	CA
Country	US
Email address	JDoe@gmail.com

If your information is incorrect, contact DMH Certificate Administrator.
tpa@dmh.lacounty.gov
213-351-1335

Continue

Legal Notices | Privacy
Copyright© 2013 Symantec Corporation. All rights reserved.

Norton SECURED
powered by VeriSign



Step 5: Click Install certificate.

Enroll: Confirm your identity | Enrollment information | **Install certificate** | Next steps

Install your certificate

When you begin certificate installation, you will see popups that warn you about potential security issues. These warnings are normal, and are part of the certificate installation process.

Review the sequence of these popups, and then click **Install certificate** to begin the process. You must have ActiveX enabled before proceeding with this installation.

- 1 Click Yes.

Web Access Confirmation

Yes No

- 2 Click Yes.

Web Access Confirmation

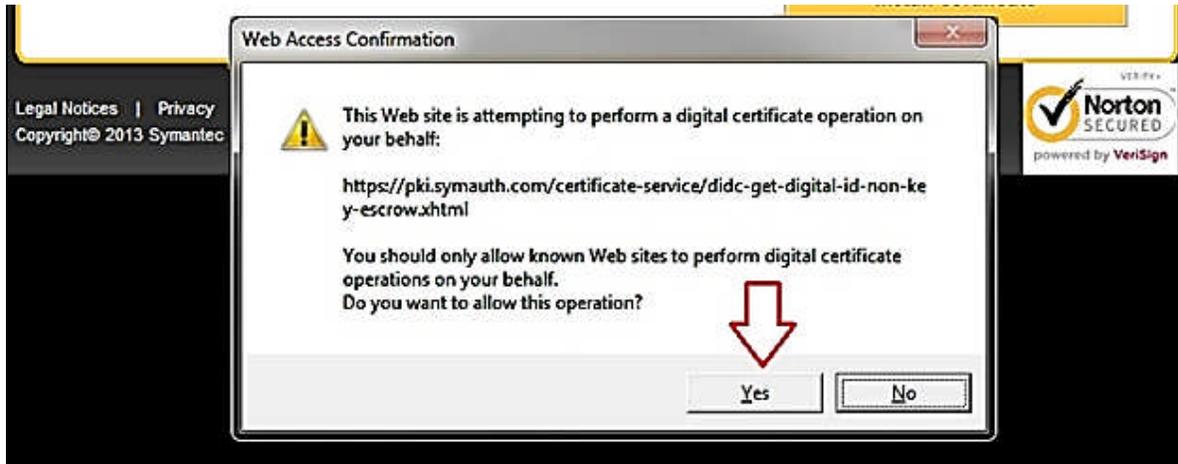
Yes No

Install certificate

Legal Notices | Privacy
Copyright© 2013 Symantec Corporation. All rights reserved.

Step 6: To confirm, click **Yes**.

Note: You'll get the same message again. Click **Yes**, to confirm it again.



Step 7: The system will show that **your certificate was successfully installed**.

- Click **additional instructions** to set up the certificate on your computer.
- Close out the **Enroll** window and follow the steps in the **additional instructions**.



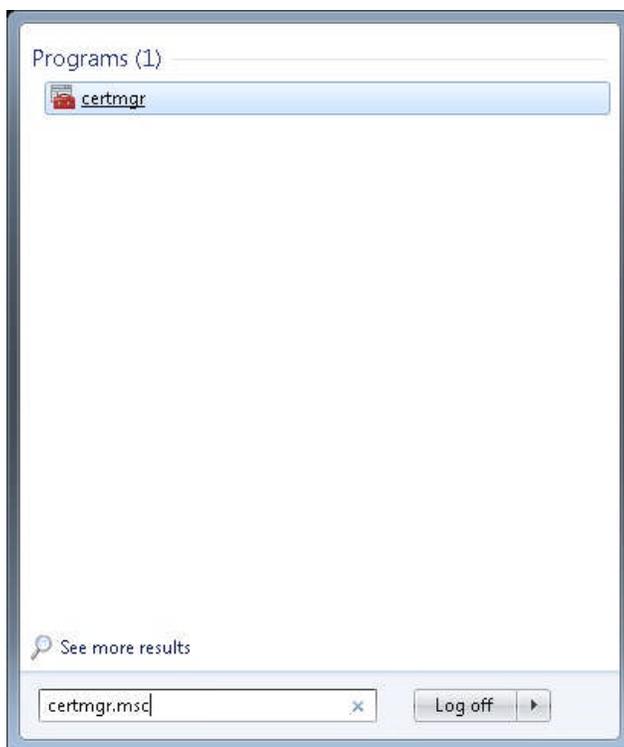
D.2 Additional Instructions (Key Set Up)

Your certificate has been installed but your computer will not trust the certificate because the issuer (Los Angeles County Department of Mental Health) is not recognized as a public trusted certification authority.

Follow the steps to install the Los Angeles County Department of Mental Health public key in order to validate the digital certificate and keys you were just issued.

Step 1: Open the Certificates Manager Console

1. For Windows 7: Click the **Start button**  and type **certmgr.msc** and press **Enter**.

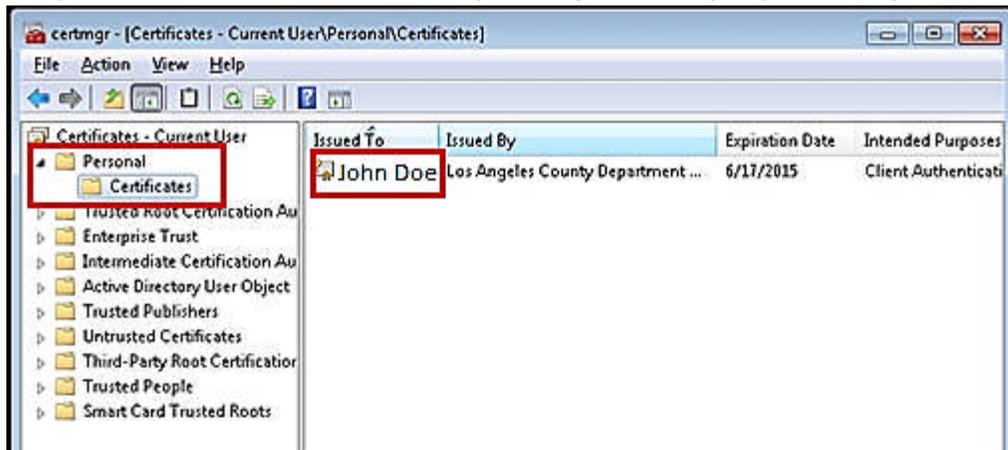


- This will open the certificate manager console.



2. Navigate to the folder **Personal\Certificates** and open the certificate by double clicking the name the certificate is issued to (the **Authorized Person** whose name was provided in the TPA Request Application).

In this example it has been issued to John Doe by Los Angeles County Department of Mental Health.



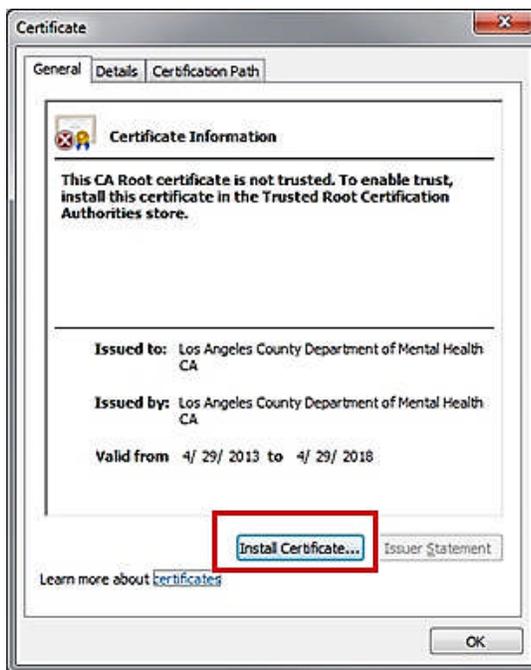
Step 2: Open the CA certificate

1. Double click the name under **Issued To** and it will open the Certification Authority certificate.
2. Once the certificate is open, click the **Certification Path** tab.
3. Click the entry **Los Angeles County Department of Mental Health CA**.
4. Click **View Certificate**.



- This will open the certificate containing the public key of **Los Angeles County Department of Mental Health CA** and indicating the CA Root certificate is not trusted.

5. Click **Install Certificate**.

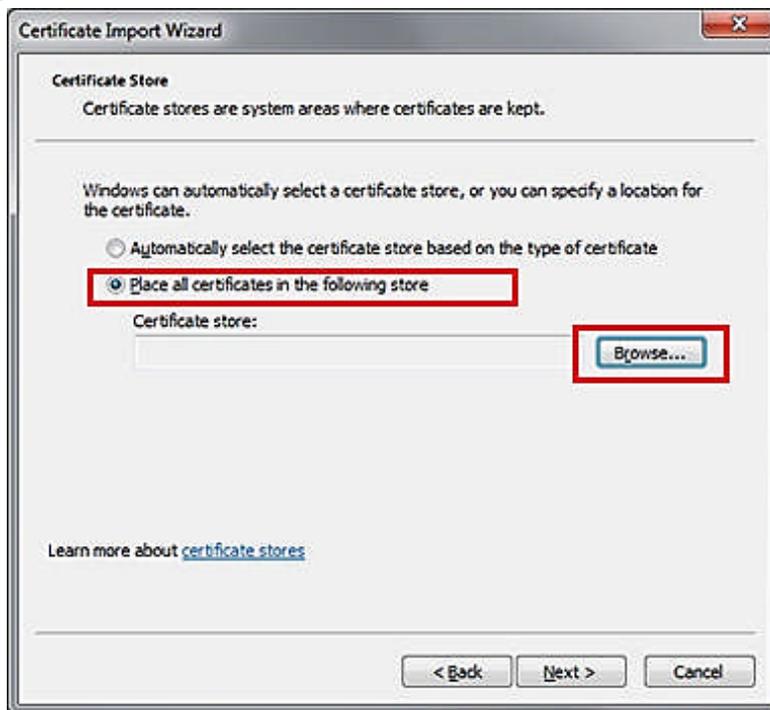


Step 3: Import the Certification Authority certificate

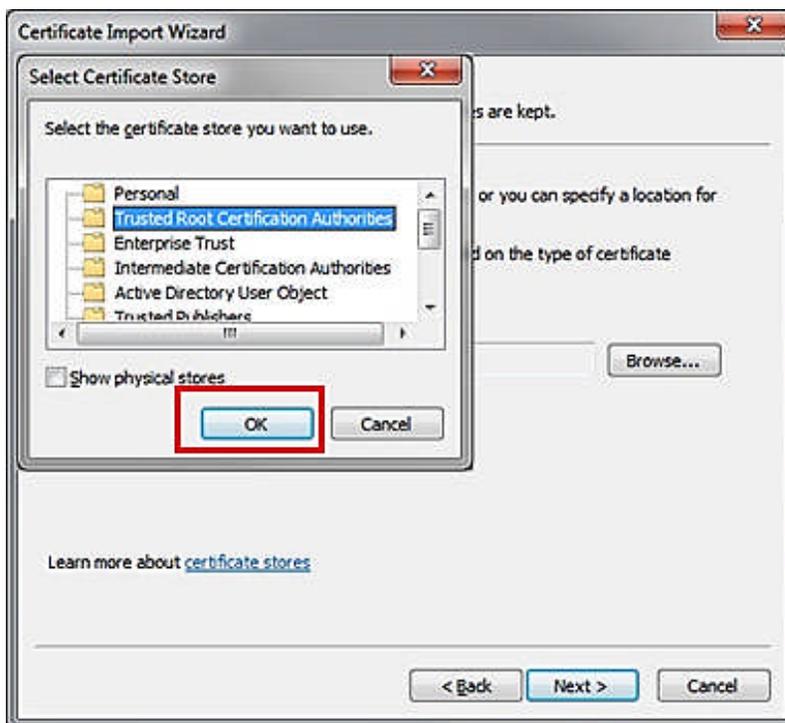
1. Click **Next**.



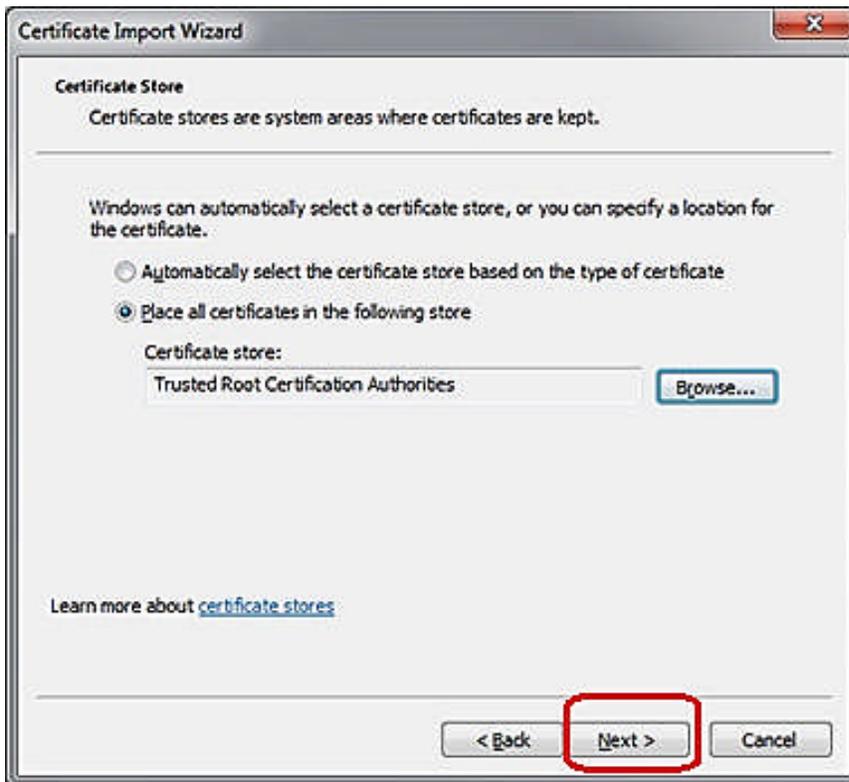
2. Select **Place all certificates in the following store** option.
3. Click **Browse**.



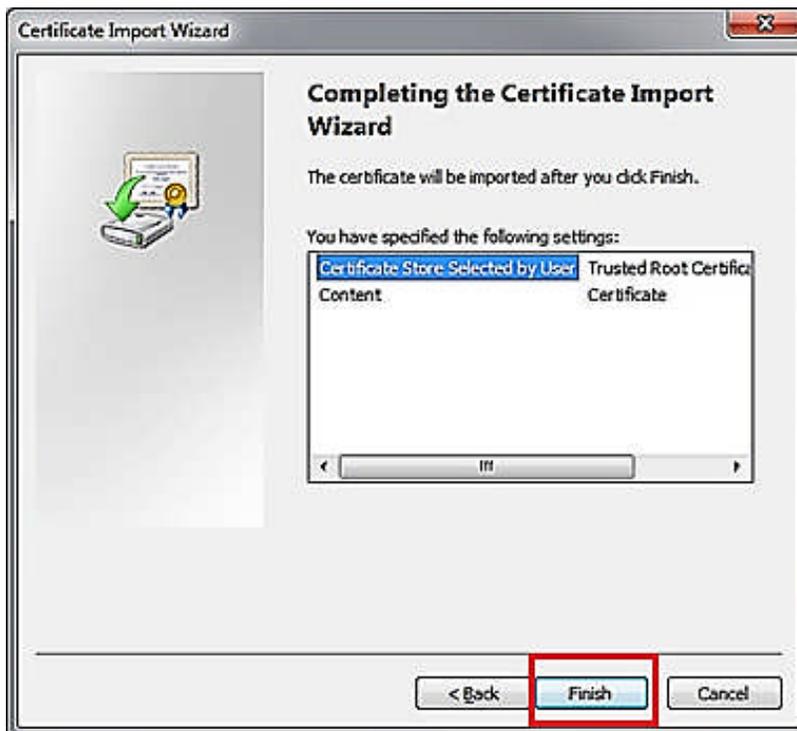
4. Select **Trusted Root Certification Authorities** folder.
5. Click **OK**.



6. Click **Next**.



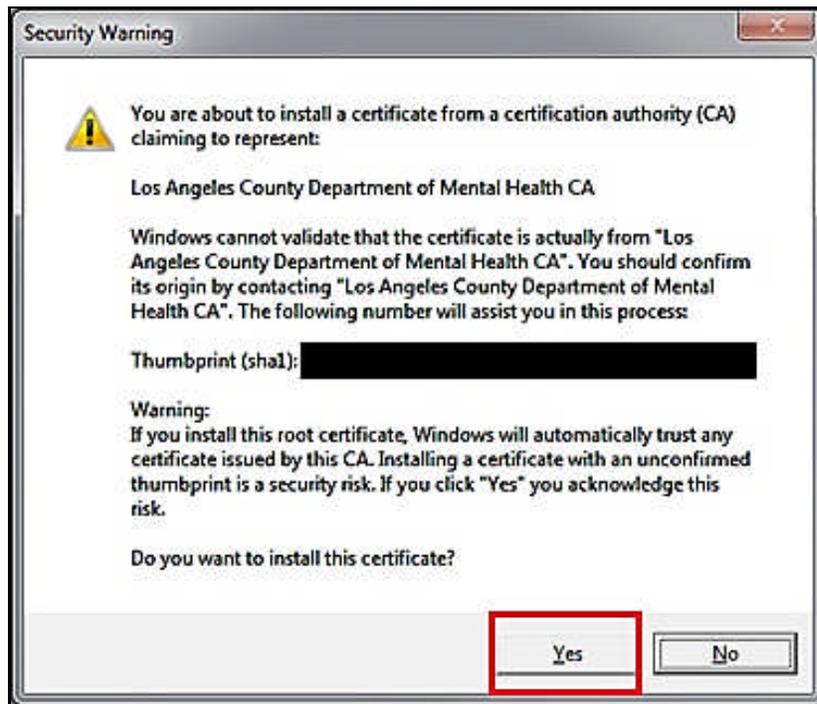
7. Click **Finish**.





The following warning should be displayed indicating that you are about to install the **Los Angeles County Department of Mental Health CA**.

- Click **Yes**.



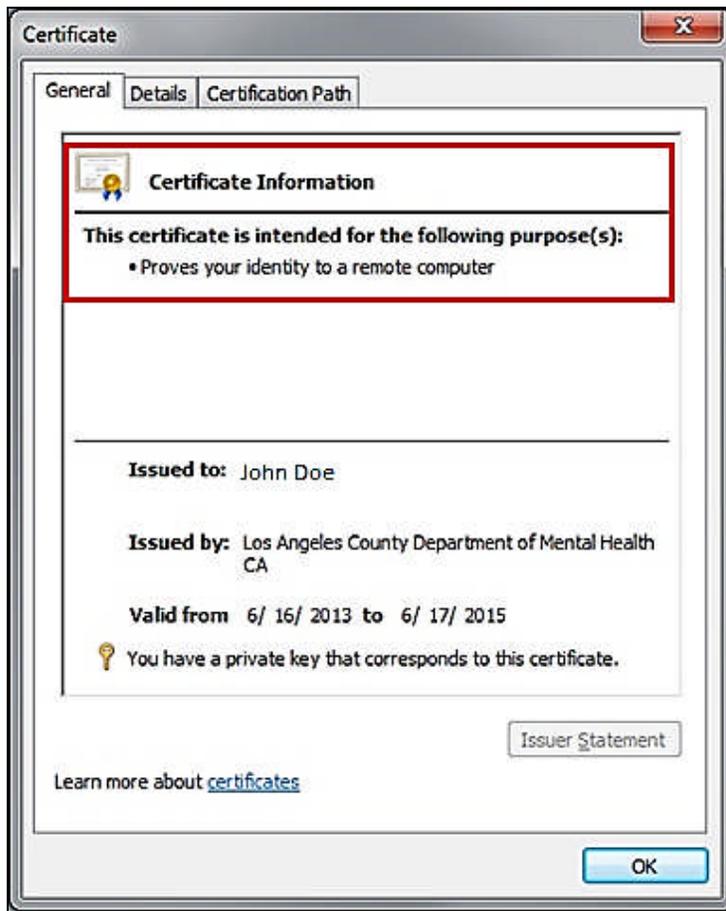
The following message should display stating “The import was successful”.

- Click **OK**.



Step 4: Verify the installation

Repeat Steps 1 and 2 to return to the Certificates Manager Console and open your certificate by double clicking the name under **Issued To**.

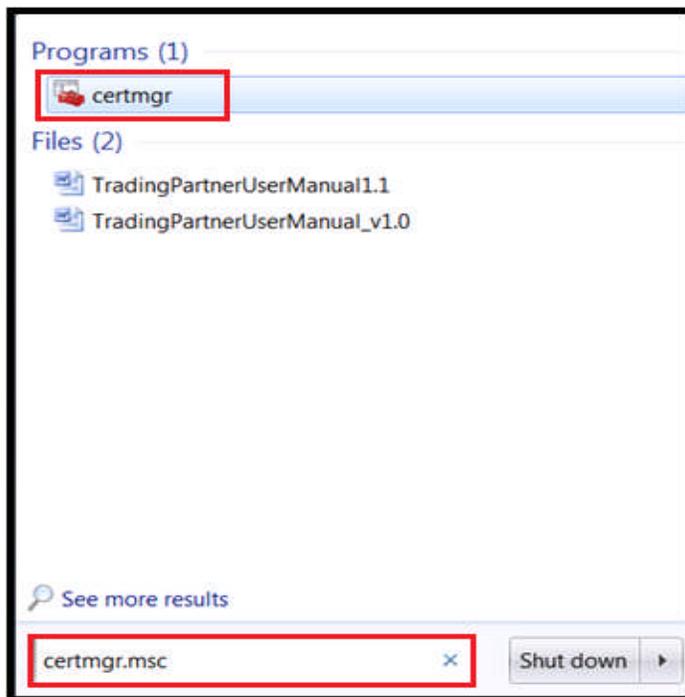


This icon  should display next to the Certificate Information section. Your computer should now be able to trust the **Los Angeles County Department of Mental Health CA** and any certificates issued by it.

Step 5: Export the certificate

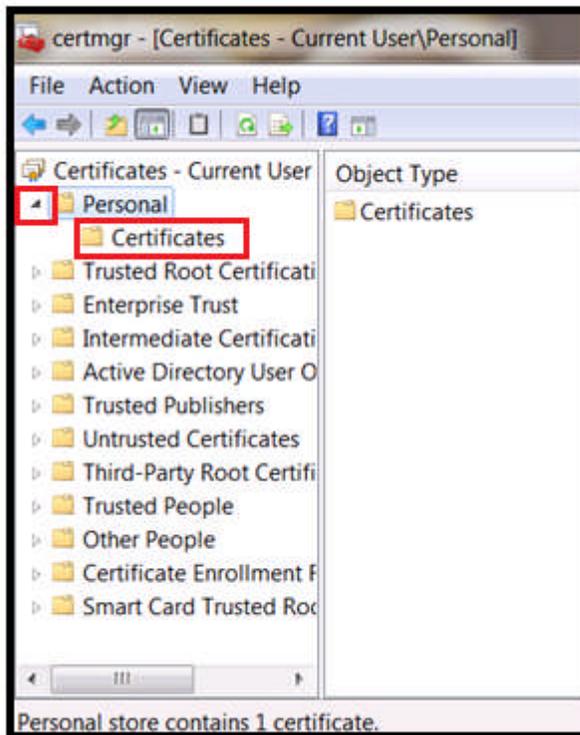
Note: It is important to retain a backup of your certificate for recovery purposes.

1. For Windows 7: Click the **Start button**  and type **certmgr.msc** and press **Enter**.

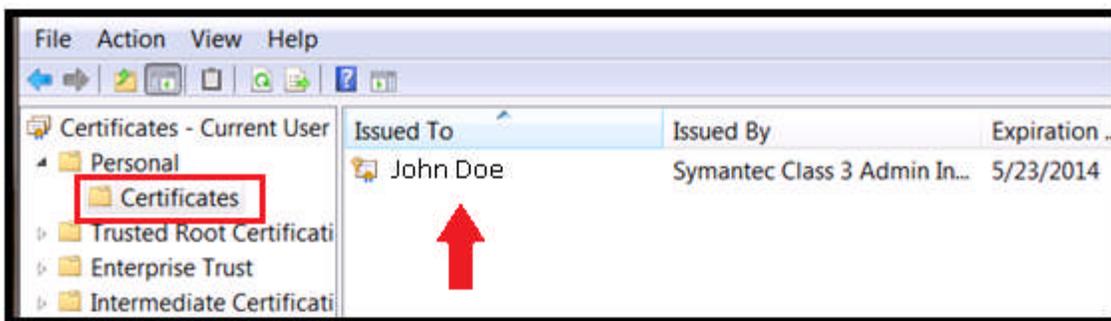


2. This will open the Certificate Manager Console.

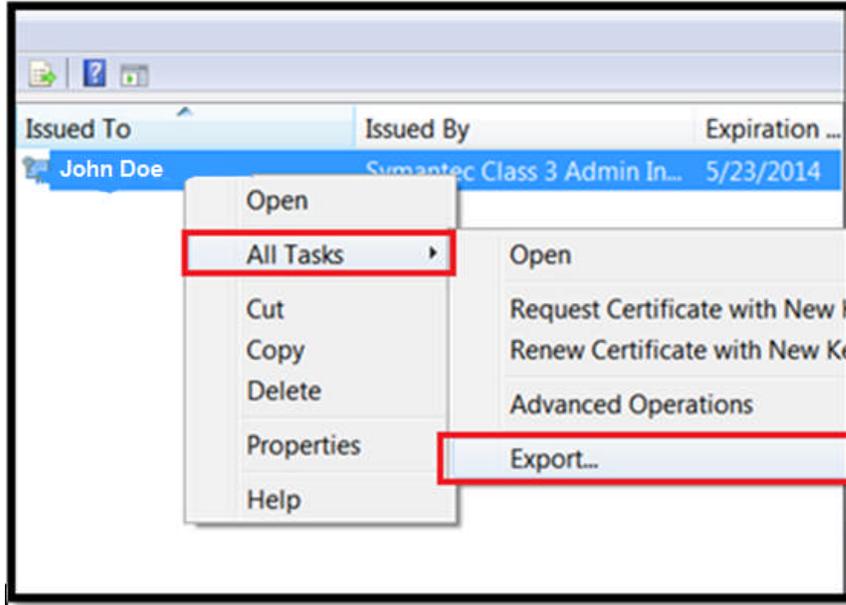
3. Navigate to the folder **Personal\Certificates**.



4. In the **Certificates** folder, locate the certificate issued by DMH.



5. Right click on the certificate.
6. Click **All Tasks**.
7. Click **Export**.



8. This will open the **Certificate Export Wizard** window.
9. Click **Next**.



Exporting Public Key

10. To export the “Public Key”, click on **“No, do not export private key”**.
11. Click **Next**.

exporting private keys'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box." data-bbox="250 199 791 588"/>

Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

Yes, export the private key

No, do not export the private key

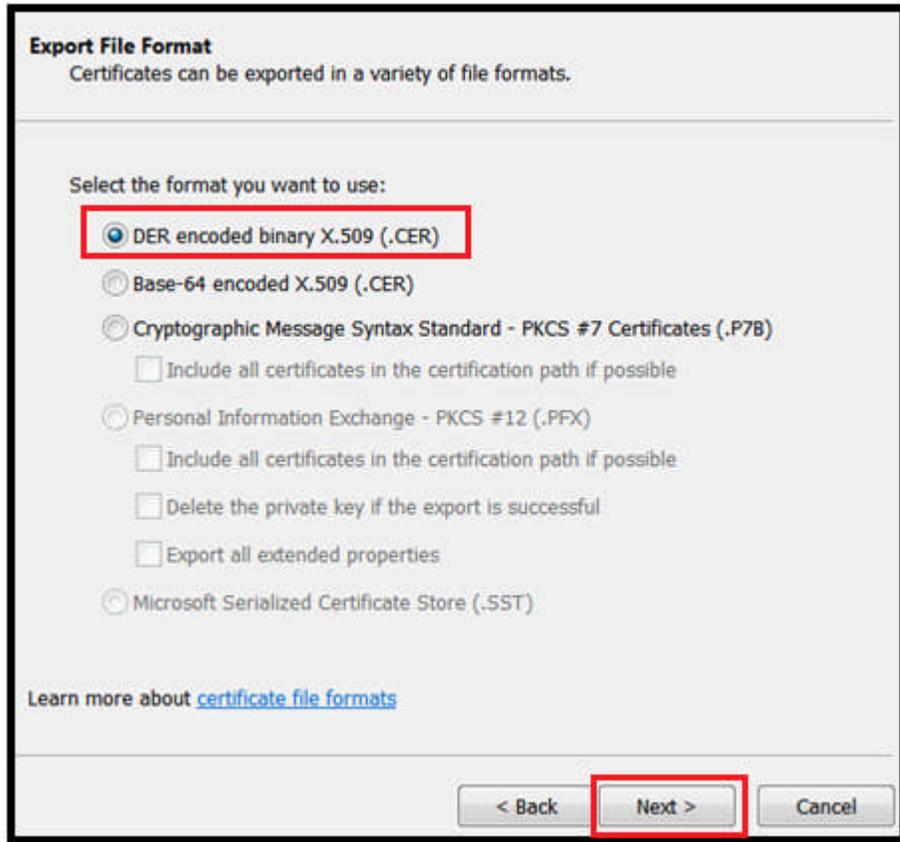
Note: The associated private key is marked as not exportable. Only the certificate can be exported.

Learn more about [exporting private keys](#)

< Back **Next >** Cancel

12. By default leave **DER encoded binary X.509 (.CER)** selected

13. Click **Next**.



Export File Format
Certificates can be exported in a variety of file formats.

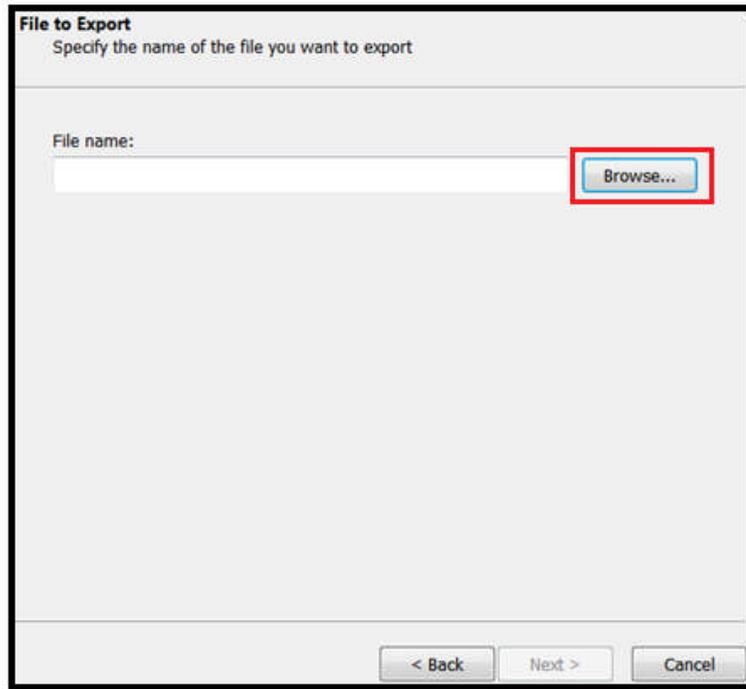
Select the format you want to use:

- DER encoded binary X.509 (.CER)
- Base-64 encoded X.509 (.CER)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
 - Include all certificates in the certification path if possible
- Personal Information Exchange - PKCS #12 (.PFX)
 - Include all certificates in the certification path if possible
 - Delete the private key if the export is successful
 - Export all extended properties
- Microsoft Serialized Certificate Store (.SST)

Learn more about [certificate file formats](#)

< Back **Next >** Cancel

14. Click **Browse** to name the file and specify location to save.

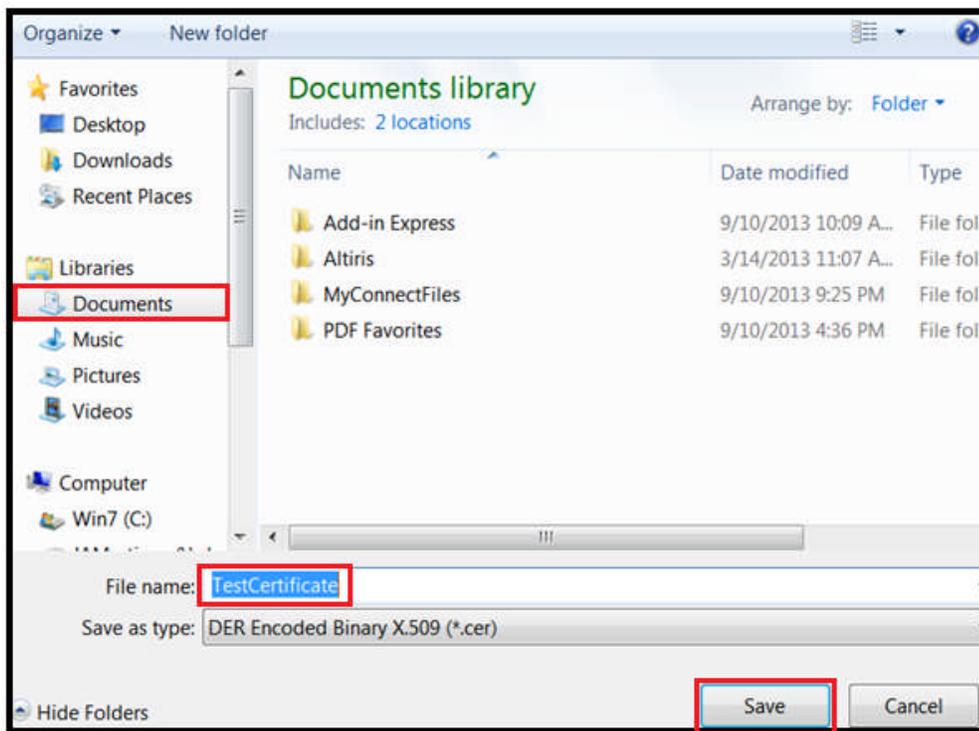


File to Export
Specify the name of the file you want to export

File name: **Browse...**

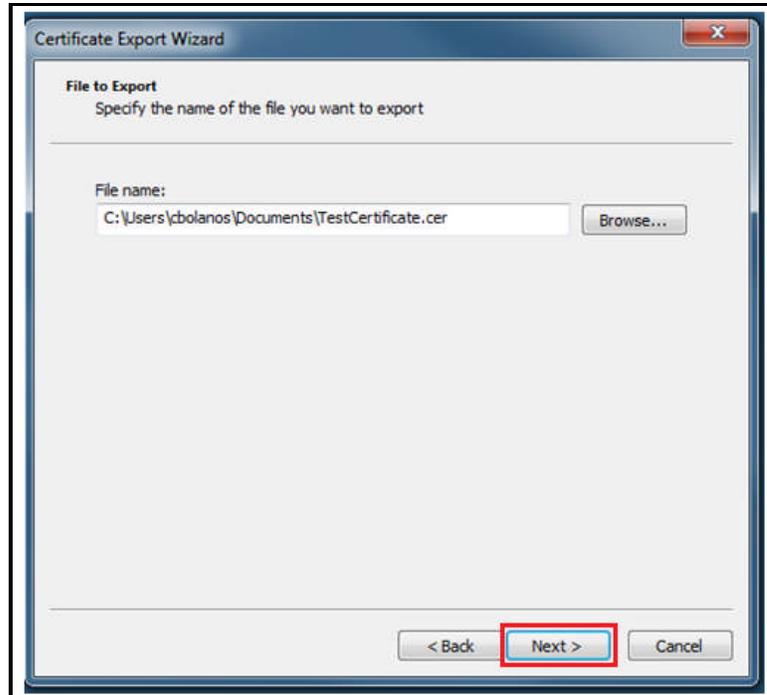
< Back Next > Cancel

15. Select a location (i.e., **Documents**).
16. Enter a **file name** for your certificate.
17. Click **Save**.

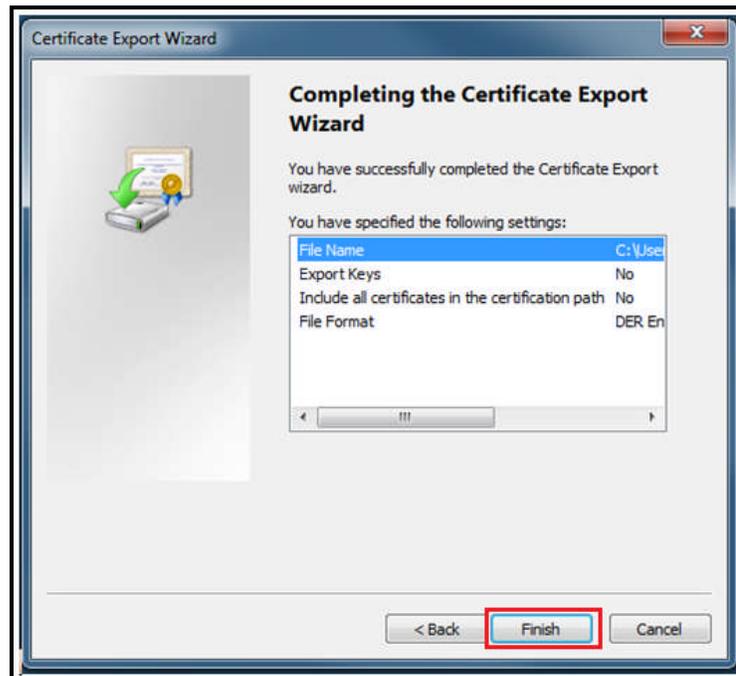


18. Verify the path where the certificate is being saved.

19. Click **Next**.



20. Click **Finish**.

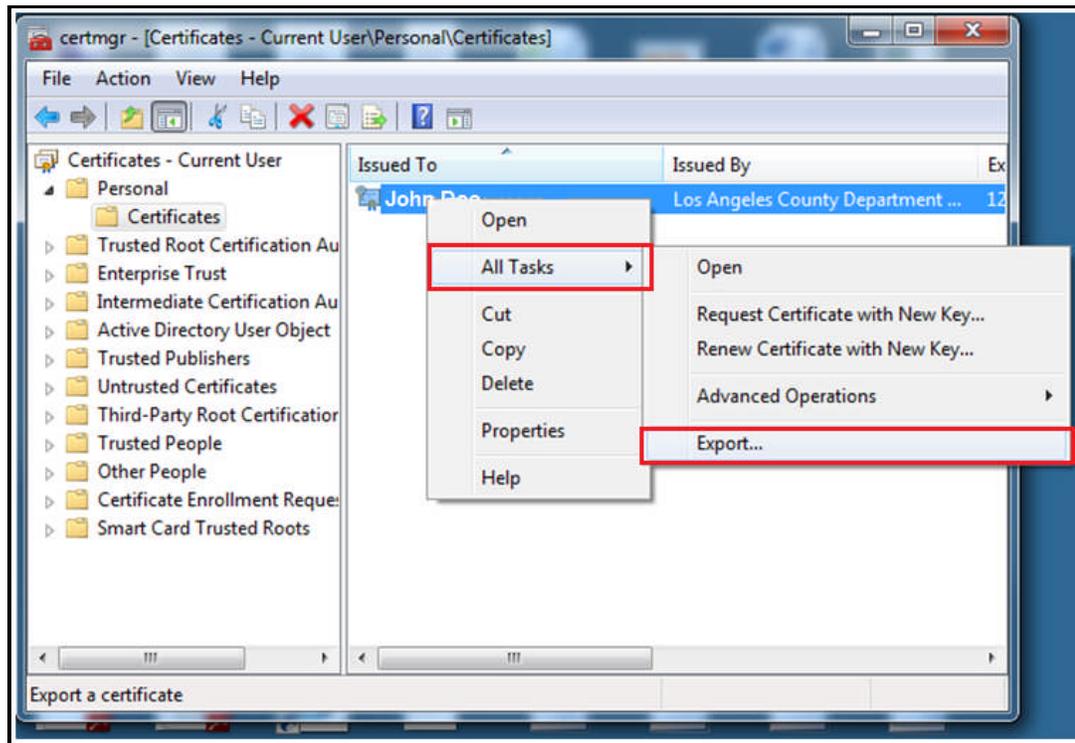


21. A message indicating that **the export was successful** will be displayed.
22. Click **OK**.

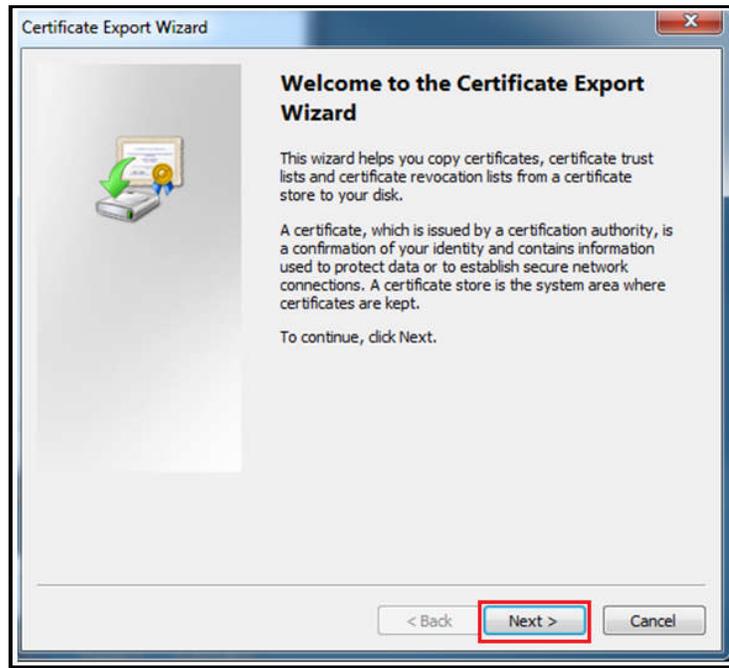


Exporting Private Key

1. To export the “Private Key”, from certmgr.msc, right click on the certificate.
2. Click **All Tasks**.
3. Click **Export**.

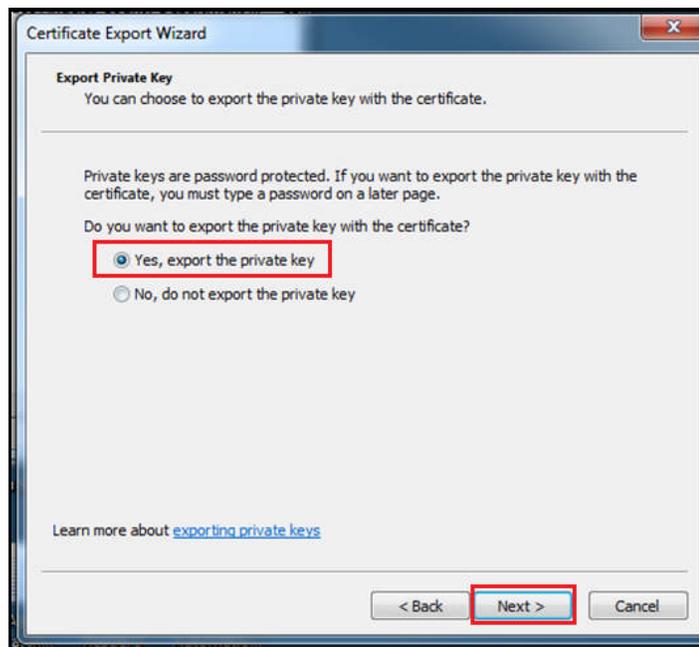


4. Click **Next**.

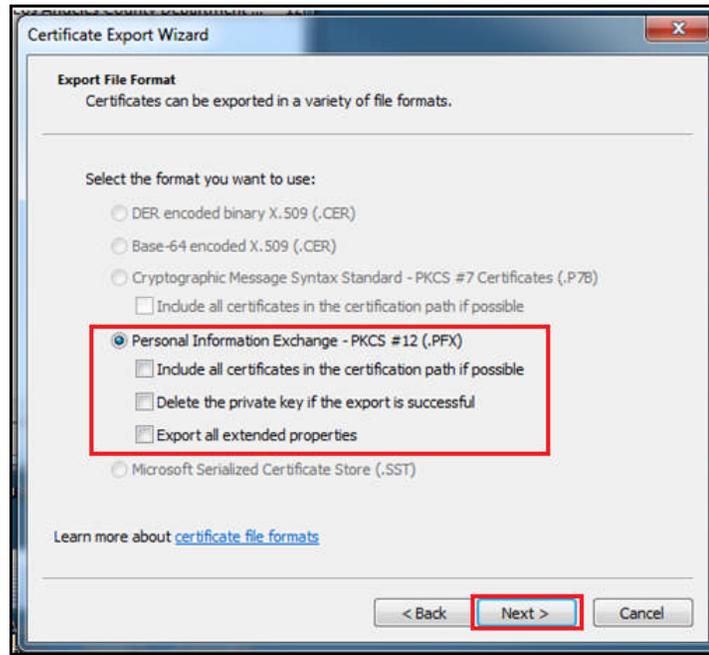


5. Click on **“Yes, export the private key”**.

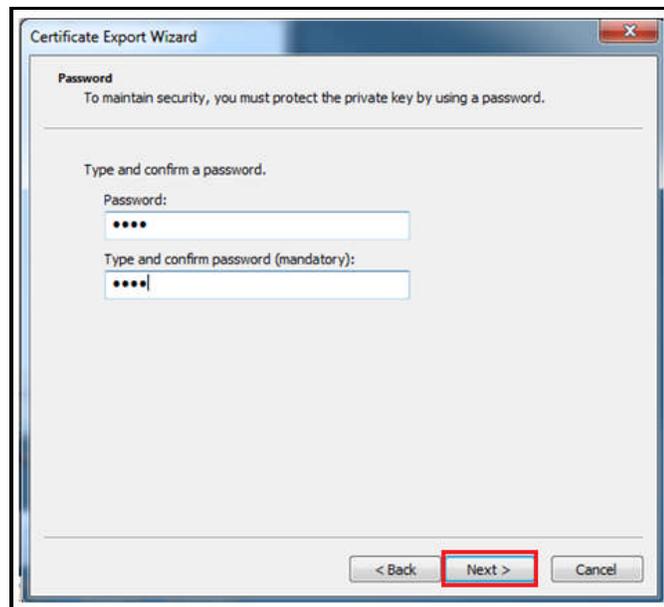
6. Click **Next**.



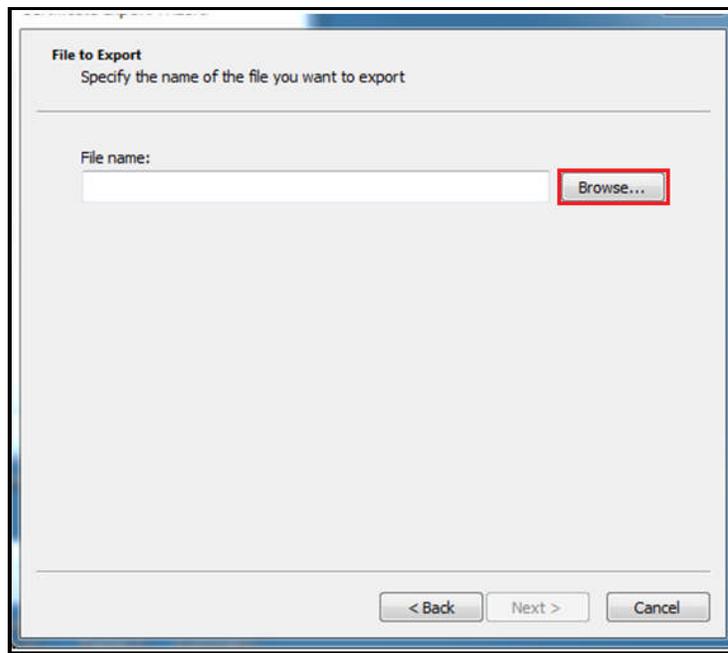
7. By default, leave **Personal Information Exchanged – PKC #12 (.PFX)** selected.
8. Leave the additional checkboxes unselected.
9. Click **Next**.



10. Create a Password for private certificate. **It is important to remember this password.**
11. Click **Next**.



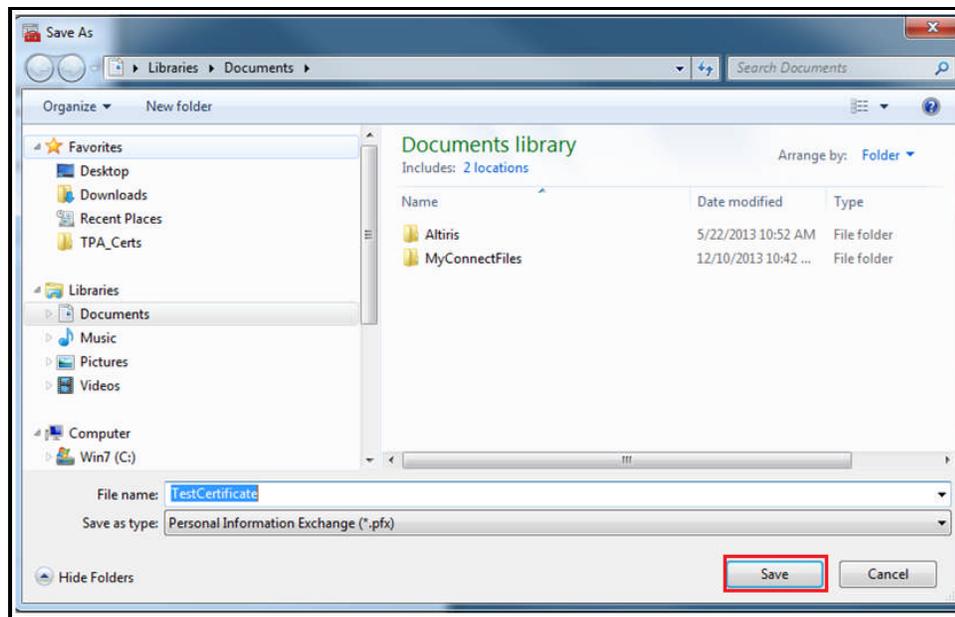
12. Click **Browse** to name the file and specify location to save.



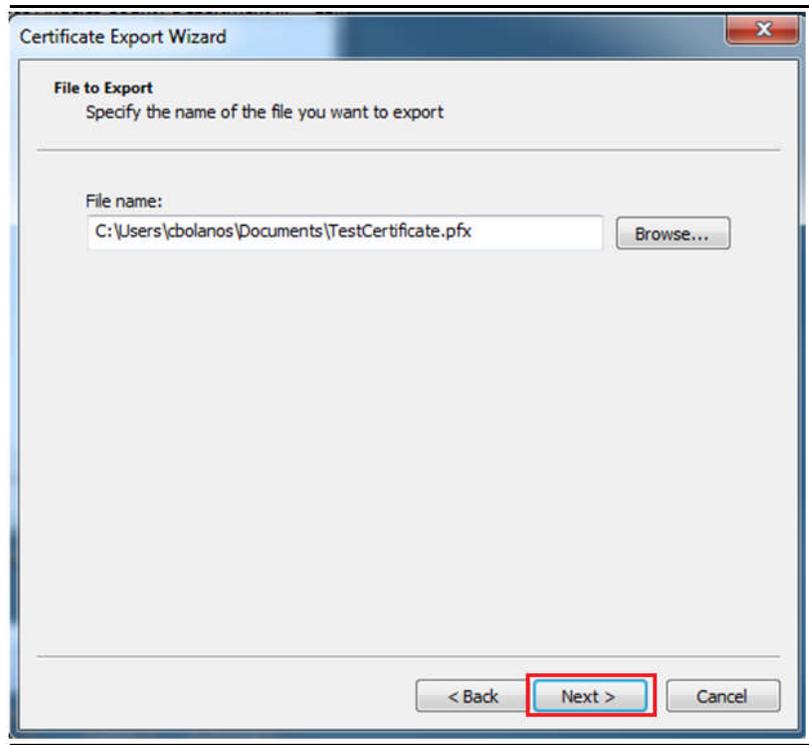
13. Select a location (i.e., **Documents**).

14. Enter a **file name** for your certificate.

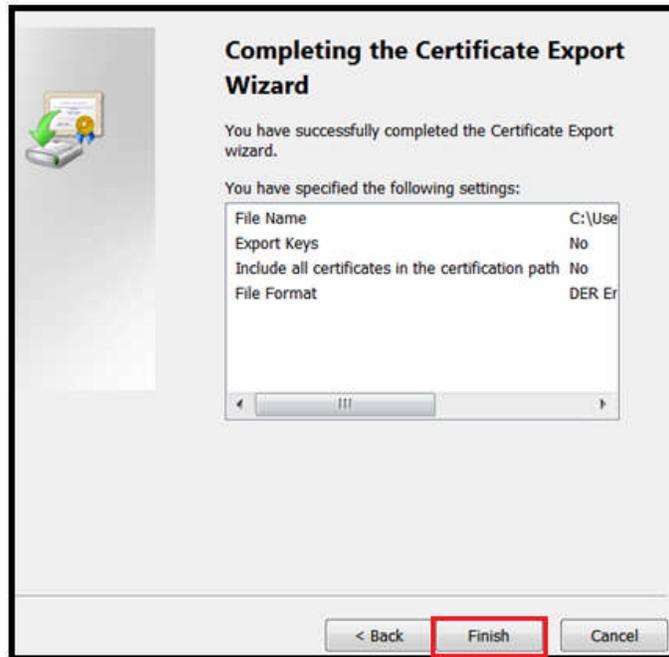
15. Click **Save**.



16. Verify the path where the certificate is being saved.
17. Click **Next**.



18. To complete the **Certificate Export Wizard**, click **Finish**.



19. A message indicating that **the export was successful** will be displayed.

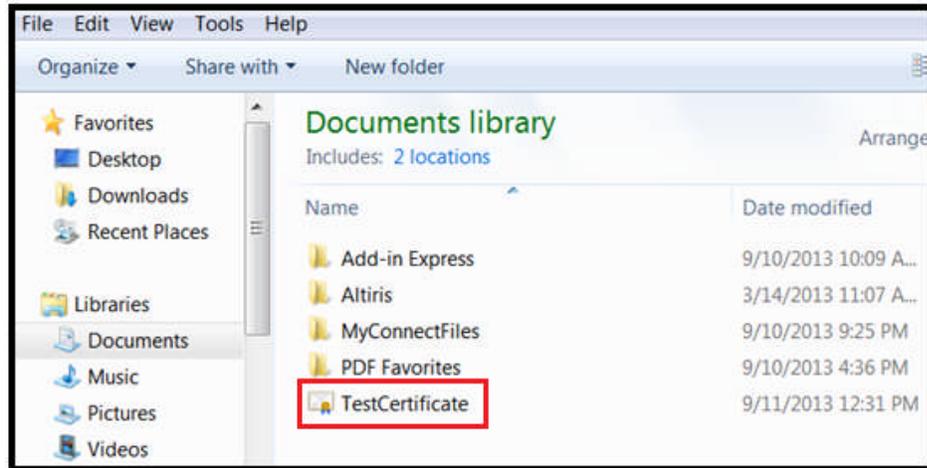
20. Click **OK**.





21. To verify that the certificate was exported, locate the folder in which the certificate is saved.

In this example, the file is located under Libraries folder/Documents.



*****DIGITAL KEY DOWNLOAD - IMPORTANT NOTICE for SYSTEM ADMINISTRATORS*****

In the event “.CER” and “.PFX” format of issued Digital Certificates doesn’t work with your current FTP Client, please follow instructions to have it converted to “.CRT” and “.KEY” format.

Locate instructions at:

Contract Providers: http://lacdmh.lacounty.gov/hipaa/IBHIS_EDI_Guides.htm

Network Providers: http://lacdmh.lacounty.gov/hipaa/ffs_IBHIS_EDI_Guides.htm

File Name: Instructions to Convert OpenSSL to PKCS

Note: The valid timeframe for a certificate is 2 years. For renewal, the Symantec MPKI system will send weekly reminders a month prior to certificate expiring to the email on file.