



# Digital Certificate Management – Back up and Configuration Guide

**Integrated Behavioral Health Information Systems (IBHIS) Project**

---

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

Version 1.0

04/24/2014



## DOCUMENT REVISION HISTORY

Version	Release Date	Revised by	Comments/ Indicate Sections Revised
Version 1.0	04/24/2014	DMH Integration Team	Release Version



## Table of Contents

A.	INTRODUCTION.....	3
A.1.	Purpose.....	3
A.2.	Disclaimer .....	3
B.	EXPORTING THE CERTIFICATE .....	4
B.1.	Accessing Certificates Manager Console .....	4
B.2.	Locating and Exporting the Certificate .....	6
C.	INSTALLING PRIVATE KEYS .....	14



## **A. INTRODUCTION**

### **A.1. Purpose**

This document describes the process by which Trading Partners can export and back up their assigned Digital Certificate for data exchange with the Los Angeles County Department of Mental Health. For assistance with initial installation, please see the **Digital Certificate Management – Initial Installation Guide**.

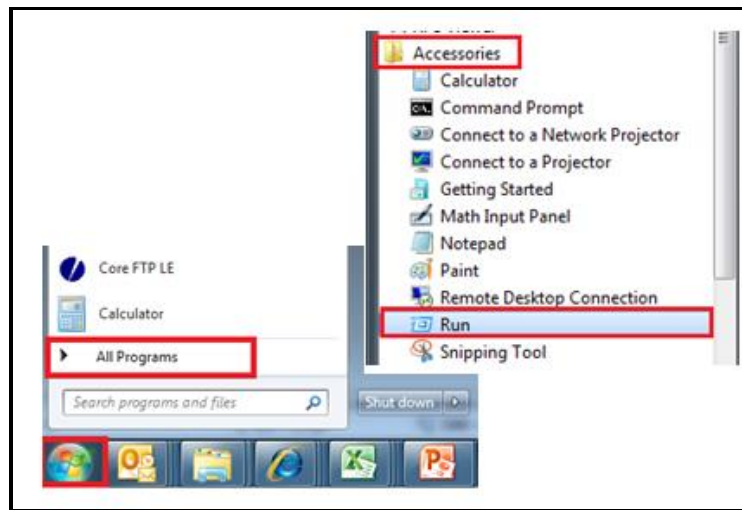
### **A.2. Disclaimer**

This guide was written for Trading Partners using a windows operating system of Windows XP or higher. If your organization is using Linux, Unix, IOS, or any other operating system, please contact your organizations Information Technology group for support.

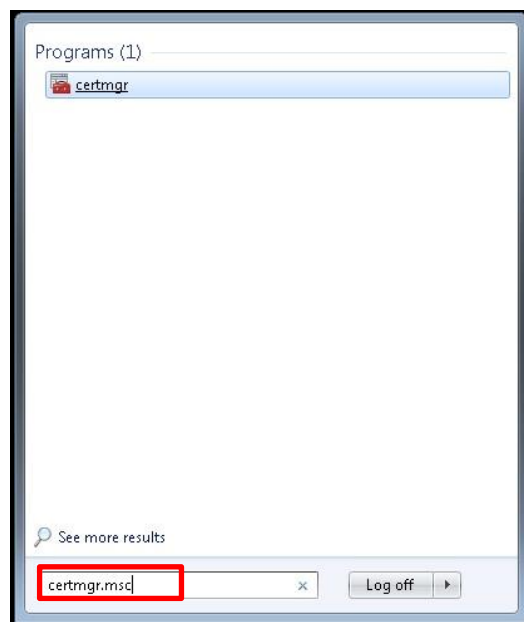
## B. EXPORTING THE CERTIFICATE

### B.1. Accessing Certificates Manager Console

1. For Windows XP or higher click the **Start** menu
2. Click **All Programs**
3. Click **Accessories**
4. Click **Run**

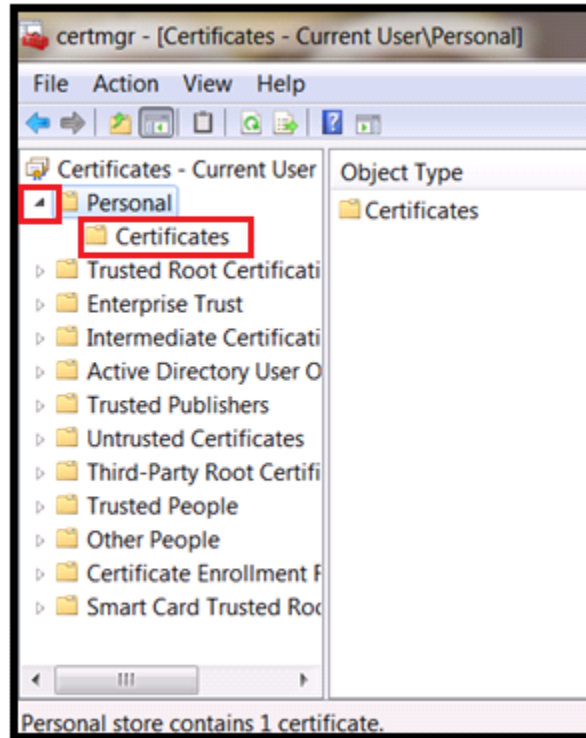


5. Type **certmgr.msc**
6. Click **Enter**



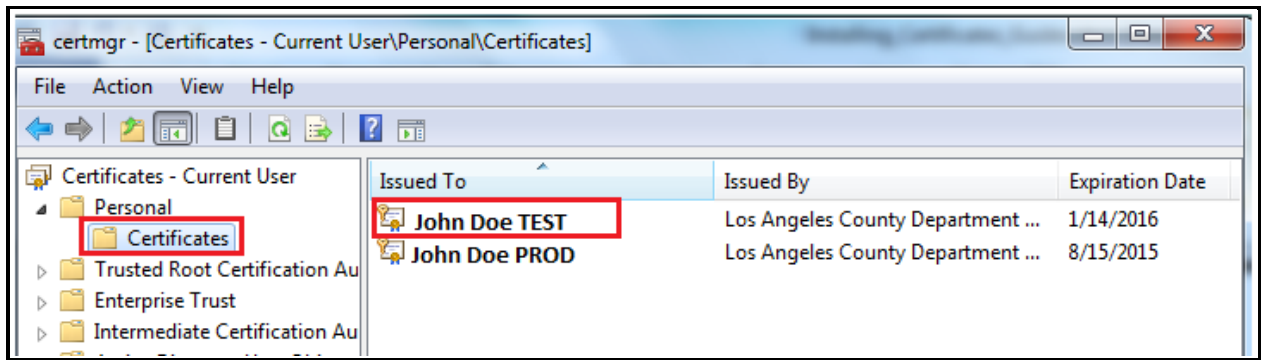
The certificate manager console will appear.

7. Navigate to the folder **Personal/Certificates** from the **Certificate Manager Console**.

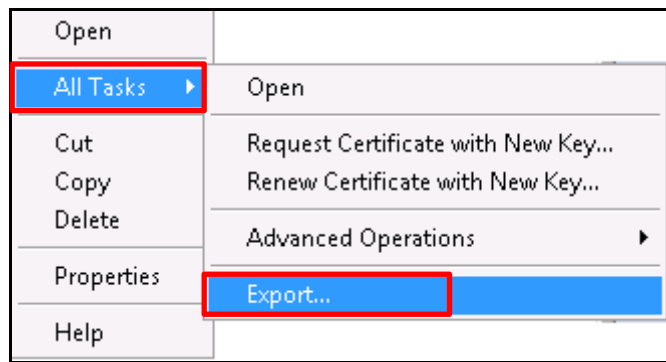


## B.2. Locating and Exporting the Certificate

1. Locate the certificate issued for TEST or Production (PROD) to your organization by Los Angeles County Department of Mental Health within the **Certificates** folder.
2. Right click the certificate (e.g., John Doe TEST)

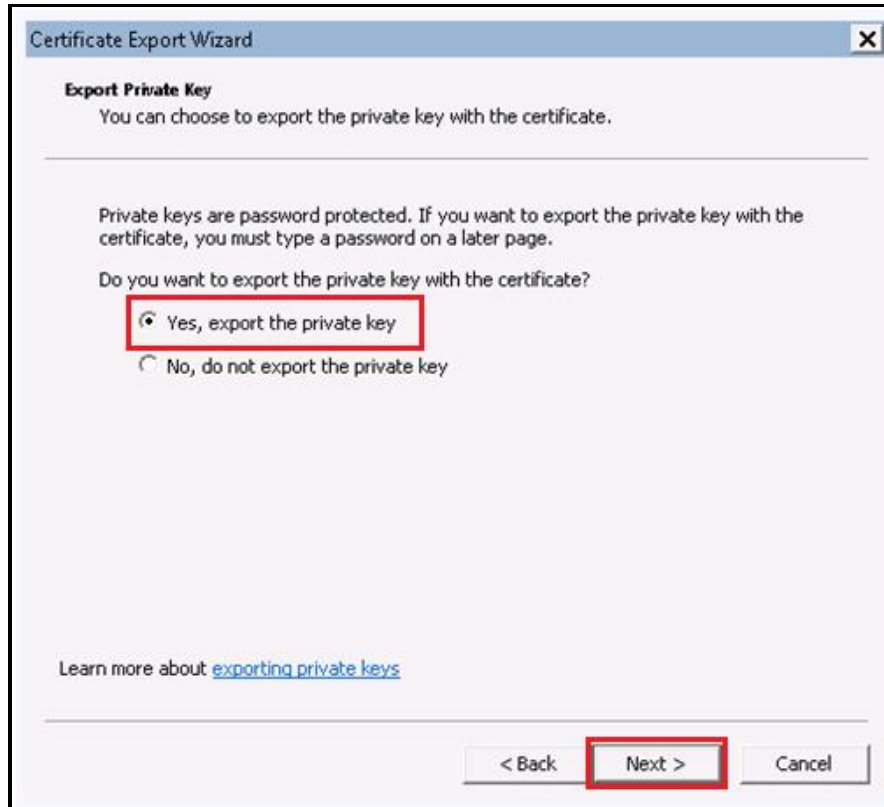


3. Click **All tasks**
4. Click **Export**



The Certificate Export Wizard will begin.

5. On the **Export Private Key** page select **Yes, export the private key**
6. Click **Next**



Certificate Export Wizard

**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

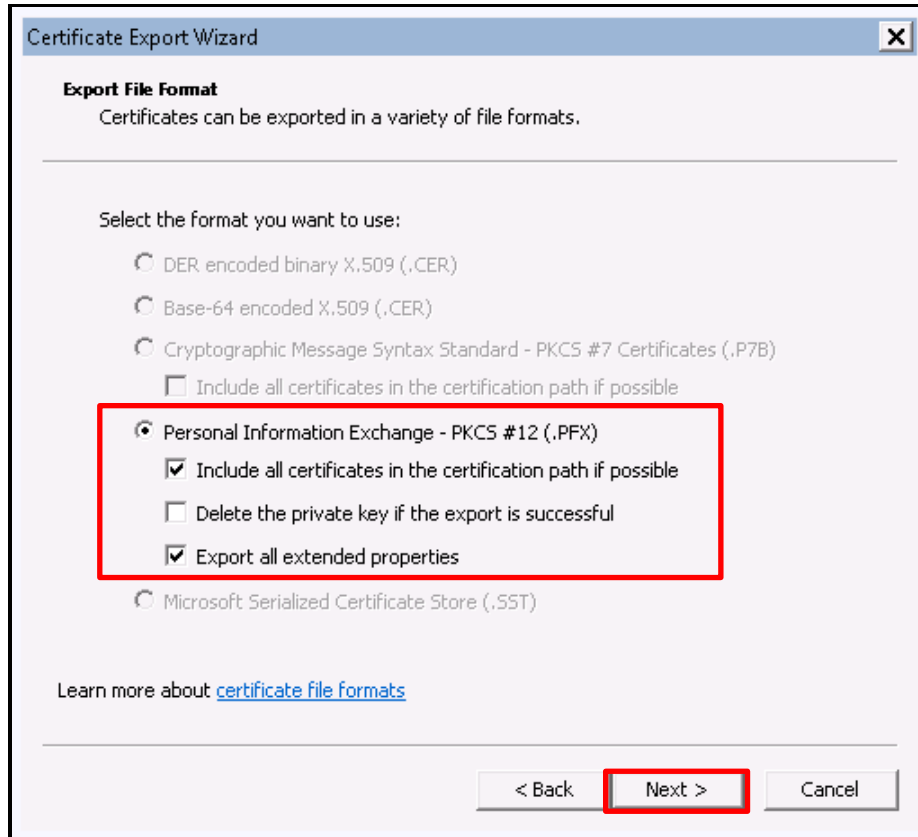
No, do not export the private key

Learn more about [exporting private keys](#)

< Back   **Next >**   Cancel



11. On the **Export File Format** page select **Personal Information Exchange**
  - a. Select ***Include all certificates in the certification path if possible***
  - b. Select ***Export all extended properties***
12. Click **Next**



Certificate Export Wizard

**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)

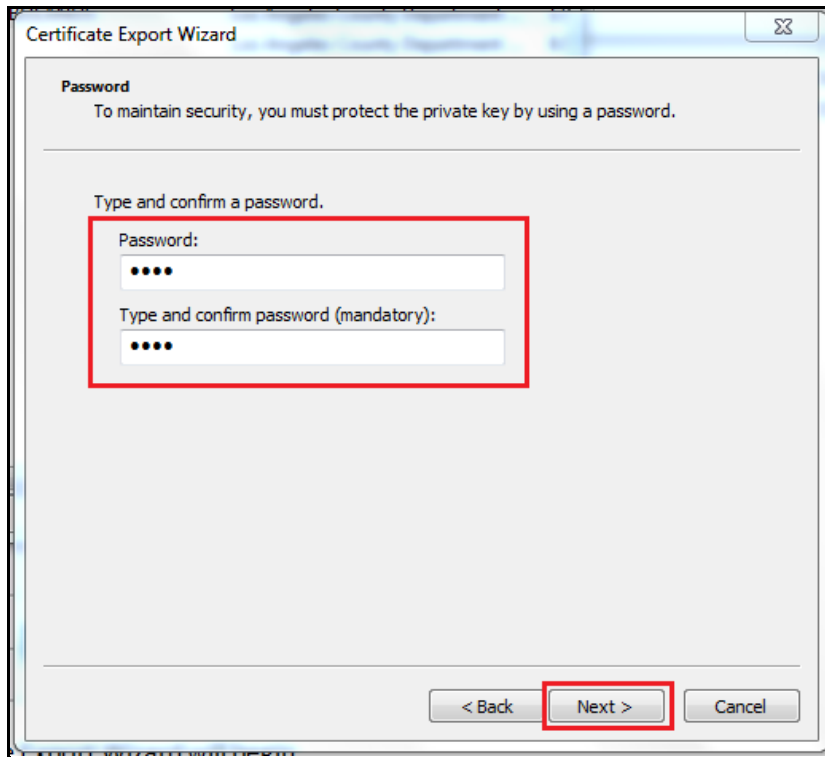
Learn more about [certificate file formats](#)

< Back   **Next >**   Cancel

**Note:** In order to successfully reinstall the exported certificate these options must be selected.

13. Enter and confirm **Password** in text boxes
14. Click **Next**

**Note:** This password will be requested anytime the exported certificate is installed, or converted to a different format.



Certificate Export Wizard

**Password**  
To maintain security, you must protect the private key by using a password.

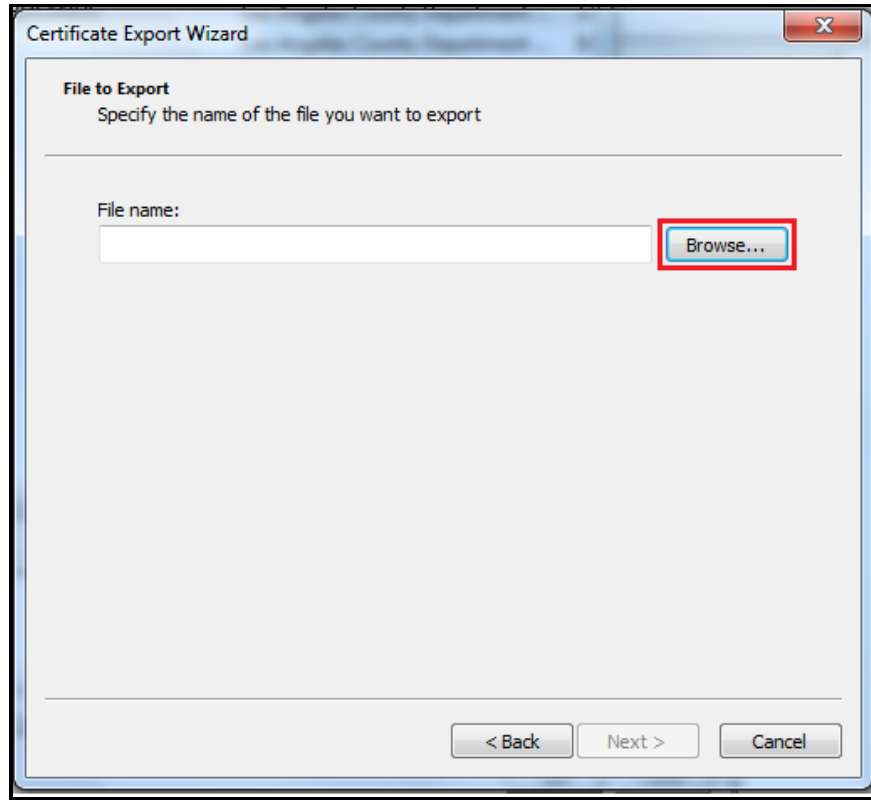
Type and confirm a password.

Password:  
••••

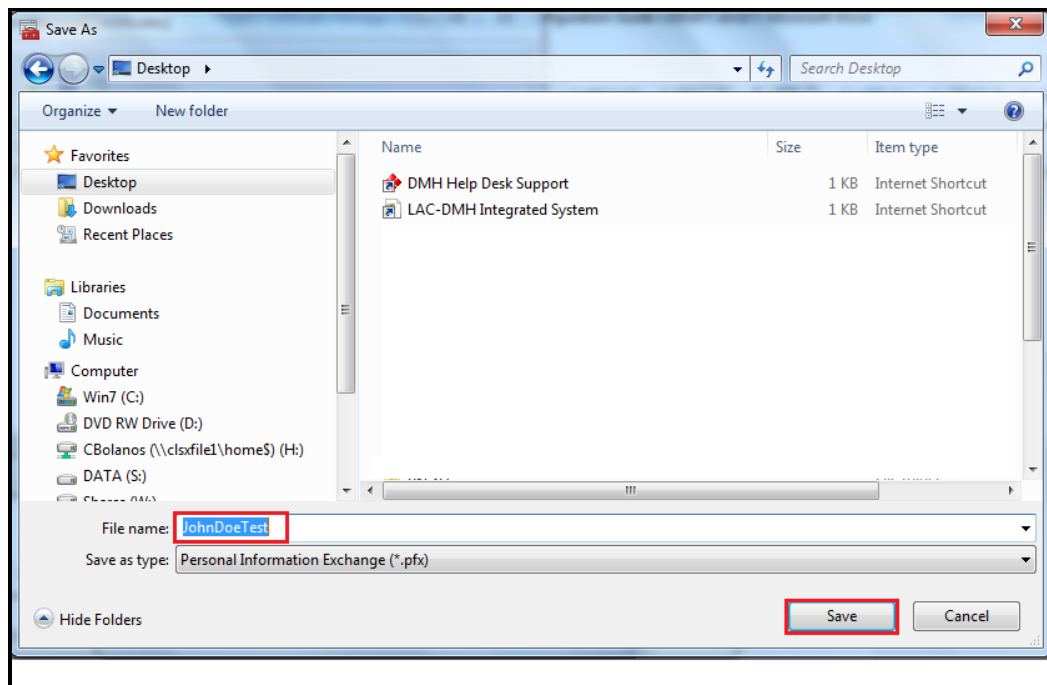
Type and confirm password (mandatory):  
••••

< Back   **Next >**   Cancel

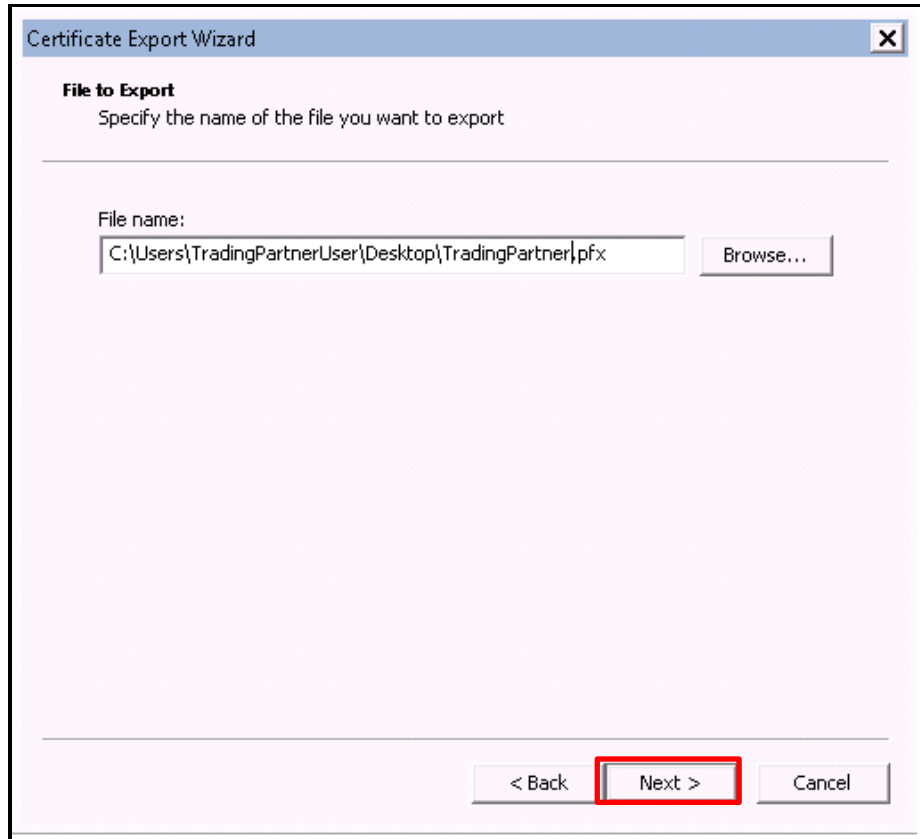
15. Click **Browse**



16. On the **File to Export** page, specify the location and file name to save the exported file.
17. Confirm the **Save as Type:** field is set to **Personal Information Exchange (.pfx)**
18. Click **Save**



19. Click **Next**

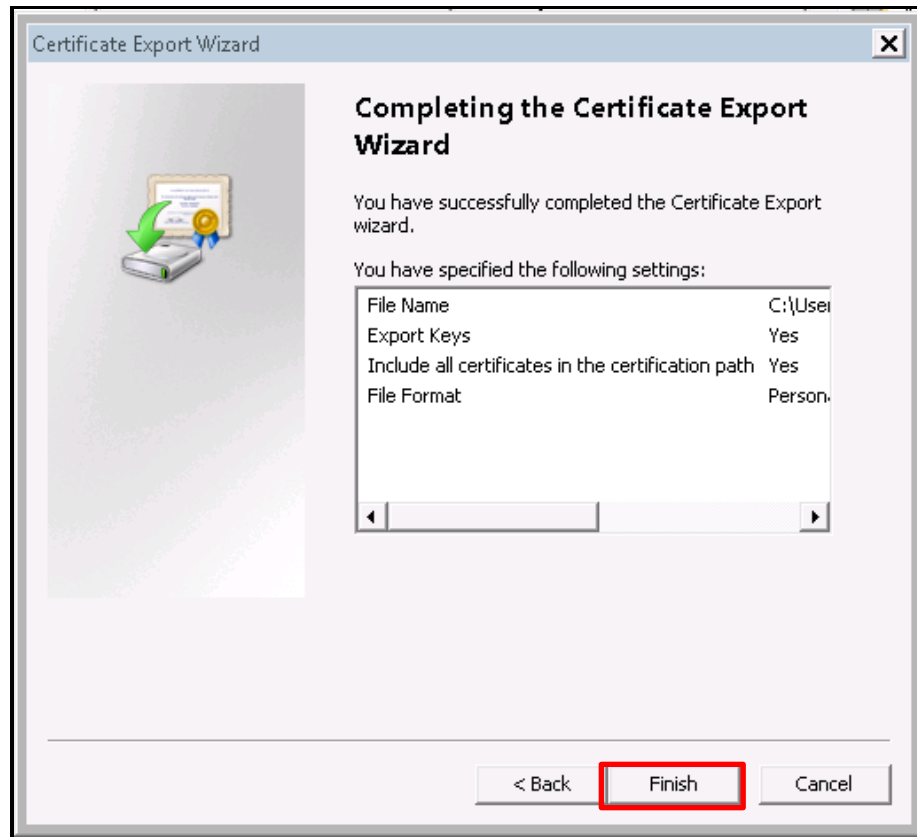


Certificate Export Wizard

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

File name:

20. Click **Finish**

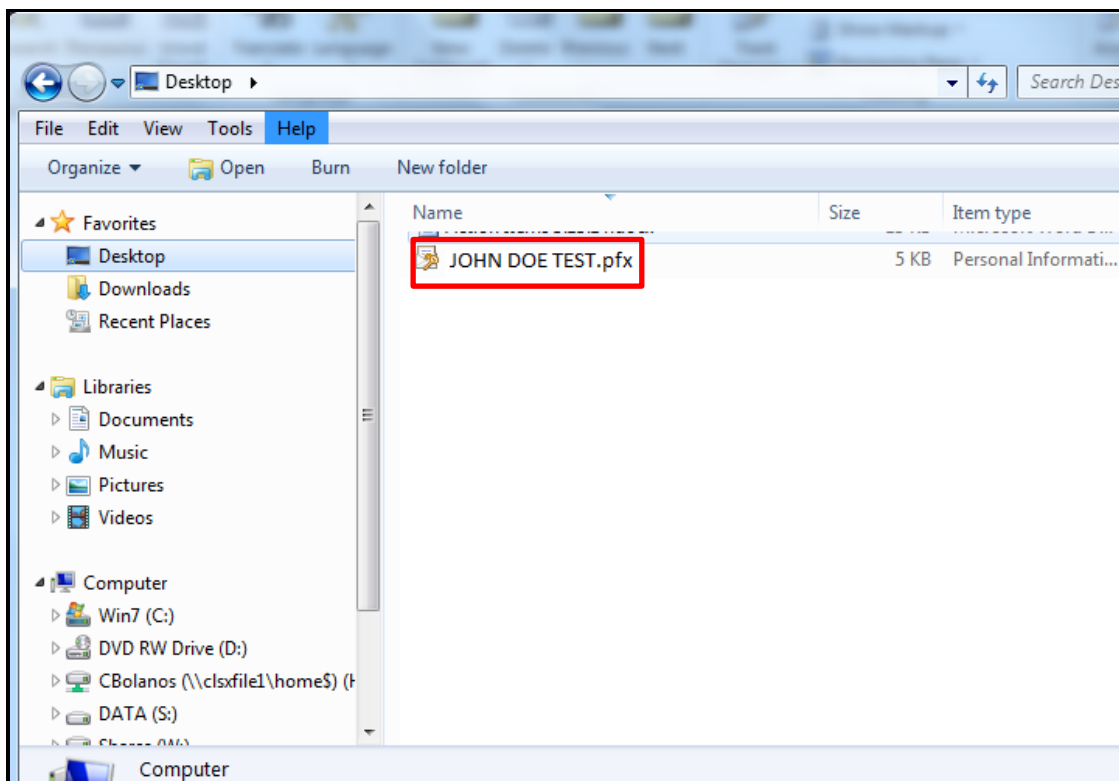


21. Navigate to the location specified and confirm the exported key.

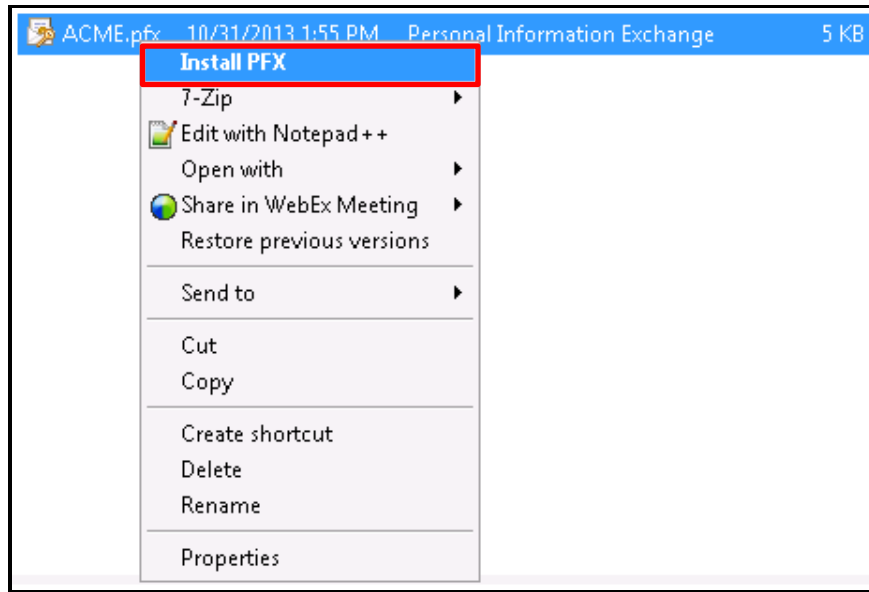
## C. INSTALLING PRIVATE KEYS

1. Navigate to the location of the Private Key
2. Right click the file

**Note:** Private Key files have an extension of .pfx, and Public Key files have an extension of .cer



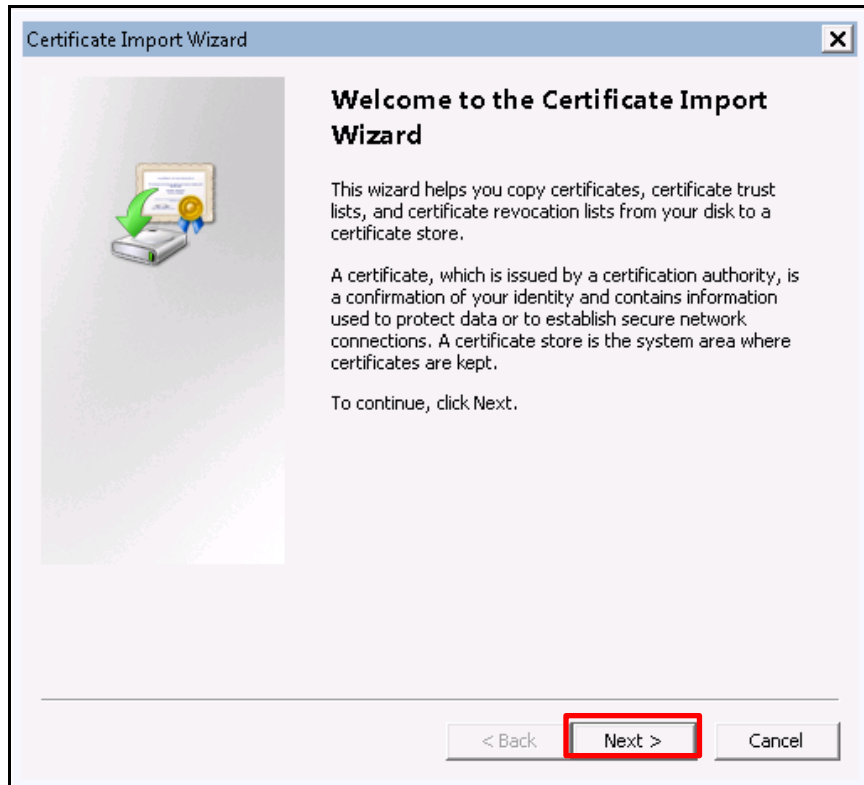
3. Click **Install PFX**



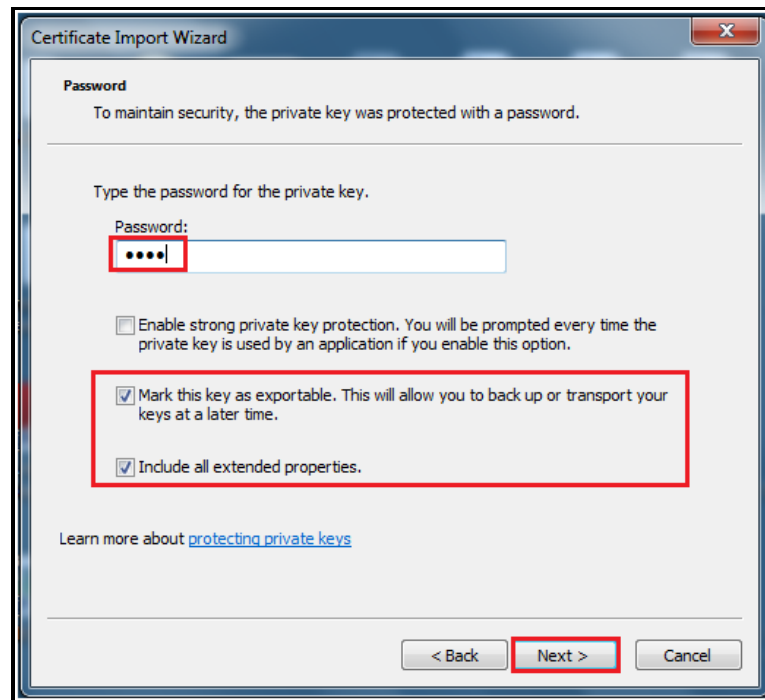


The Certificate Import Wizard will begin

4. Click **Next**



5. On the **File to Import** page, verify that the path to the key is correct. If the path is incorrect, click **Browse** and navigate to the correct key file.
6. Click **Next**
7. On the **Password** page, enter the password used to export the key file.
8. Click **Next**



Certificate Import Wizard

**Password**

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:  
.....

Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

Include all extended properties.

Learn more about [protecting private keys](#)

< Back   Next >   Cancel

**Note:** The settings above affect certificate behavior in the following ways:

- The *Enable strong private key protection...* option **requires the password every time** the certificate is used.
- The *Mark this key as exportable...* option enables the private key to be **backed up** from the machine where it is being installed.
- The *Include all extended properties* option enables extended properties to persist after reinstallation of the certificate.

For more information on Importing Certificates and Certificate Extended Properties, please refer to the following articles:

[http://msdn.microsoft.com/en-us/library/windows/desktop/aa376523\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa376523(v=vs.85).aspx)

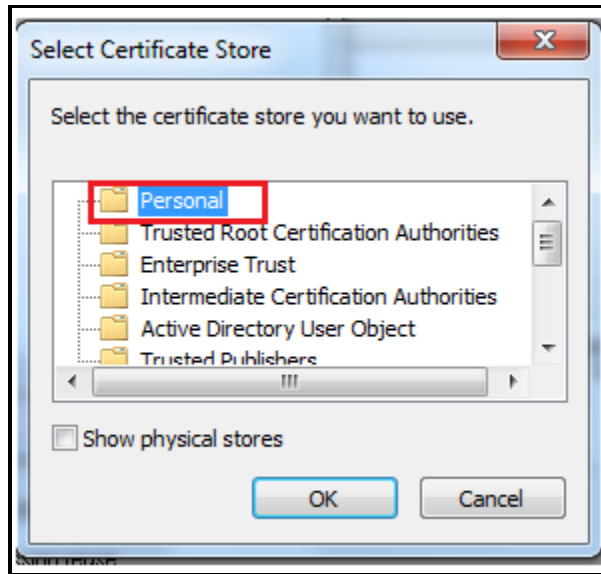
[http://technet.microsoft.com/en-us/library/cc776889\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc776889(v=ws.10).aspx)

9. Select **Place all certificates in the following store**

10. Click **Browse**



11. Select **Personal** folder



12. Click **Finish**

