

# **GUIDELINES**

## **Electronic Reporting for Ozone-Depleting Substances**

### **Part 1: Register as a CDX User**

**March 2008**

If you questions about electronic reporting, please contact:

Mike James  
Stratospheric Protection Division  
United States Environmental Protection Agency  
(202) 343-9192  
[james.mike@epa.gov](mailto:james.mike@epa.gov)

Staci Gatica  
Stratospheric Protection Division  
United States Environmental Protection Agency  
(202) 343-9469  
[gatica.staci@epa.gov](mailto:gatica.staci@epa.gov)

Jennifer Bohman  
Stratospheric Protection Division  
United States Environmental Protection Agency  
(202) 343-9548  
[bohman.jennifer@epa.gov](mailto:bohman.jennifer@epa.gov)

# Contents

---

Contents.....	3
Overview.....	4
I. Registering for CDX and Signing the Digital Signature Agreement .....	6
II. Obtaining a Digital Certificate and Digital Signature .....	10
APPLICATION STAGE .....	10
AUTHENTICATION STAGE .....	12
RETRIEVAL STAGE .....	13
III. Downloading/Exporting your Digital Certificate .....	20

## Overview

This document, **Register as a CDX User**, is the first part of a comprehensive Three-Part Guidance developed to assist you in submitting your ODS data electronically. In its entirety, the Three-Part Guidance Document provides step-by-step instructions to:

1. **Register as a CDX User**,
2. Prepare Data for Submission, and
3. Submit ODS Data to EPA.

**Part 1 of the guidance walks you through the steps of registering as a CDX user and setting up your system for ODSTS e-Reporting.** This is a one-time registration process that you will need to complete the first time you submit your data electronically. Part 2 assists you in preparing your data for submission. Part 3 guides you through the process of zipping, encrypting, and sending your files to EPA using CDX.

A number of security measures are taken to safeguard user access and identity, so various passwords, passphrases, and verification numbers are created during the process. For this reason, the document provides guidance as you maneuver through the various steps. It is important to remember your passwords and keep track of verification numbers provided to you. You should refrain from clicking on “remember password” at any of the password creation stages. This impairs database protection and the registration process can fail to verify passwords if the box is checked.

You will see there are numerous steps in this section of the guidance. Don't be afraid – the steps are very simple. Although registration is easy and your part only takes approximately twenty minutes, it will take several days for the CDX Helpdesk to verify the information and complete the registration process. It may take the CDX Helpdesk up to 48 hours to complete this step; this does not require action on the part of the user.

Please keep the CDX Helpdesk phone number on hand as you register as a CDX user. There may be slight variations in screenshots or pop-ups you encounter during the registration process. You can call the Helpdesk if you have difficulties. **[CDX Helpdesk: 1-888-890-1995]**

Here is a quick overview of the steps included in Part 1 of this guidance.

**CDX Registration** - First you will register with CDX and create a username and password. You will use this password each time you log onto the CDX system to submit your electronic forms.

**Application for a Digital Signature** - After registering with CDX, you will:

1. Submit an agreement to obtain a digital signature;
2. Register with IdenTrust (the company that specializes in identity authentication systems and issues digital signatures) to obtain your digital signature;
3. Create a passphrase for your digital signature (which is different from your CDX password); and
4. Wait for an e-mail from the CDX helpdesk informing you that your application has been approved.

A digital signature is your handwritten signature in electronic format, and provides authentication.

**Downloading the Digital Signature** - You will receive an email confirmation from the CDX with your activation code. With this code in hand, you will return to the IdenTrust web site. You may be prompted to adjust certain security settings on your computer. You will then enter your activation code and passphrase to retrieve the digital signature. After this, you will then download the digital signature to your computer. You will also create a password that you will use each time you apply your digital signature.

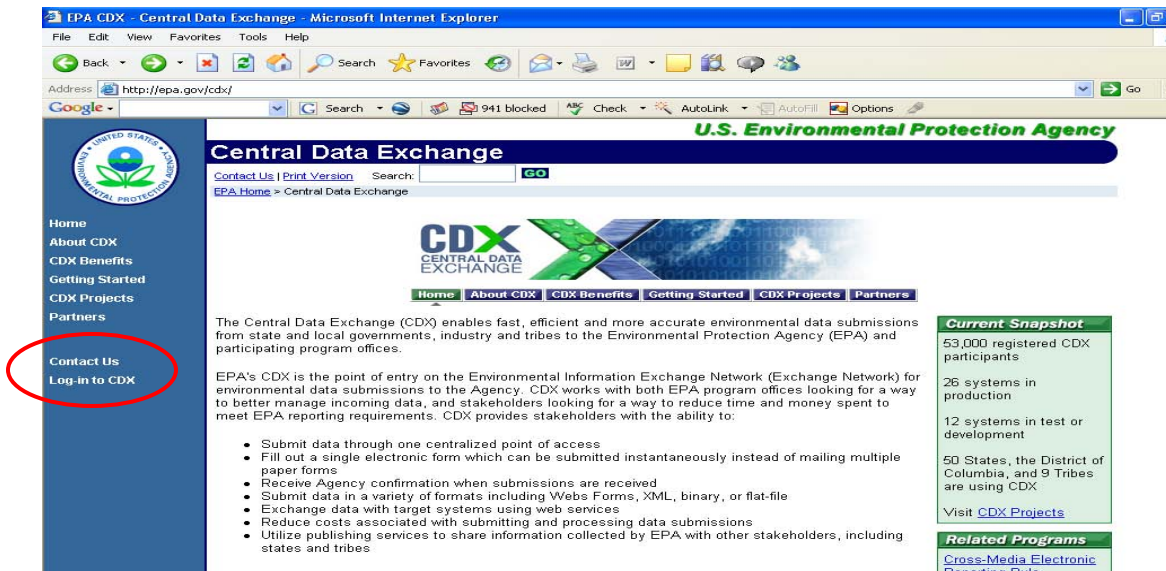
The remainder of this document discusses each of these major steps in further detail.

# I. Registering for CDX and Signing the Digital Signature Agreement

First, you should register as a CDX User.

## Step 1: Access CDX at the link: <http://epa.gov/cdx>

- Click on Log-in to CDX (on the left sidebar)



## Step 2: Click on Registration (on the left sidebar)

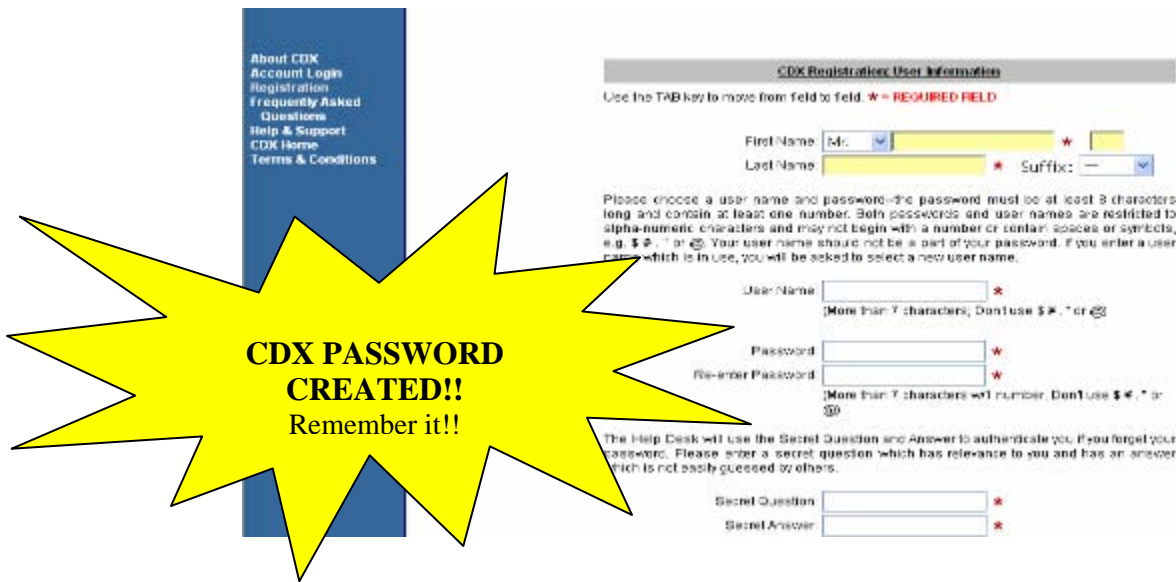


## Step 3: Read the Warning Notice and Privacy Statement and click to **continue**

**Step 4: Carefully read the Terms and Conditions and click I Accept to continue**

**Step 5: Fill out the registration information boxes and choose a password**

- Keep Password Secure. Follow the instructions provided on the CDX Website if the password is compromised. (CDX support # 1-888-890-1995)
- At the bottom of the page, select **Next** to continue



The screenshot shows the 'CDX Registration: User Information' form. A large yellow starburst with the text 'CDX PASSWORD CREATED!! Remember it!!' is overlaid on the left side of the form. The form fields include: First Name (with a dropdown menu), Last Name, Suffix (with a dropdown menu), User Name, Password, Re-enter Password, Secret Question, and Secret Answer. A navigation menu on the left lists: About CDX, Account Login, Registration, Frequently Asked Questions, Help & Support, CDX Home, and Terms & Conditions.

**Step 6: Enter Organization Information and click Next to continue**



The screenshot shows the 'U.S. Environmental Protection Agency Registration' page. The form is titled 'CDX Registration: Organization Information'. It includes fields for: Organization Name, Registrant's Work Mailing Address 1, Registrant's Work Mailing Address 2, City, State/Province (with a dropdown menu showing 'Alabama'), Zip/Postal Code, Country (with a dropdown menu showing 'UNITED STATES'), E-mail, and Phone Number. A note at the bottom states: 'U.S., Canada & Caribbean Islands Phone Format: xxx-xxx-xxxx'. A navigation menu on the left lists: About CDX, Account Login, Registration, Frequently Asked Questions, Help & Support, CDX Home, and Terms & Conditions.

## Step 6a: Click the oval to the right of Ozone Depleting Substances (ODS)

- Make sure the **oval** is highlighted and click **Next** to continue

## Step 7: On the Add Program ID page, enter N/A into the box designated for the ID #

- Make sure that the pull down screen indicates that you are a **submitter** and that the submission method indicates **Webform**
- Click **Finished**

The screenshot shows the U.S. Environmental Protection Agency's registration interface. The page title is "Registration" and the user is logged in as "0A5C200212". The main heading is "CDX Registration: Add Program ID". Below this, there is a form with the following fields:

- Rate: A SUBMITTER (dropdown menu)
- Program ID Type: ODS (dropdown menu)
- ID: N/A (text input field with a red asterisk indicating it is required)
- Submission Method: WEBFORM (dropdown menu)

A red oval highlights the "FINISHED" button. Below the form, there is a message: "You are in an encrypted secure session." At the bottom, there is a "Help Desk" link and a "Last updated" date of October 7, 2005.

## Step 7a: You are finished with the online portion of CDX registration. Read the screen and click Finished. A digital signature agreement will be automatically generated.

- The Ozone Depleting Substances Program requires **approval** for use of the dataflow, so your access to ODS will be on **hold** until approved by Mike James at the EPA.
- Your Ozone Depleting Substances account will be activated upon approval.



## II. Obtaining a Digital Certificate and Digital Signature

Now you begin the process for obtaining your digital signature. There are three steps to the applications process: 1) Application, 2) Authentication, and 3) Retrieval.

### APPLICATION STAGE

#### Step 10: Apply with ACES in order to obtain a Digital Signature

- Read the introduction page and click on **Next**



#### Step 10a: Read and click Next

#### Step 10b: Provide your e-mail address and your organization's postal code (zip code)

#### Step 10c: Enter the information for your Organization's Headquarters

- You may be prompted to select the appropriate entry from a list if your organization is already contained in the system.

#### Step 10d: Enter your Mailing Address

#### Step 10e: Enter your Employee Information

**Step 10f: Create a Passphrase for your digital signature: Remember this Passphrase and keep it in a secure location**

ACIS Business Representative Certificate Application  
CRM# NO: 3090-0272

DIGITALSIGNATURE™  
an Idemtrus™ One

**Completing Your Application**

**Your Passphrase**  
A passphrase is required to retrieve, renew or revoke your digital certificate, as well as to update your information, please create your passphrase below. You will need to enter it twice to ensure you typed it correctly.

Enter your passphrase

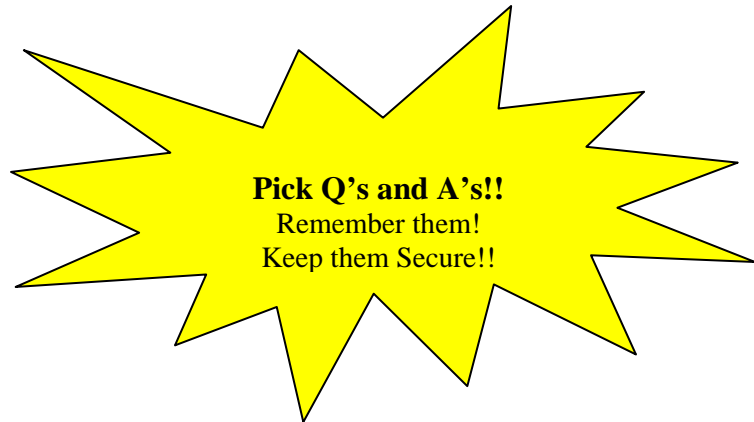
Re-enter your passphrase

Note: Your passphrase must be 8-30 characters in length and may contain letters, numbers and some special characters, and is case sensitive.

Cancel < Back | Next >



**Step 10g: Choose three questions that you will use in case you forget your Passphrase (Questions will change for each new user)**



**Step 10h: Provide easy-to-remember answers to the questions you've selected**

**Step 11: Review your information and make sure it is correct. Click Next**

**Step 12: Read the privacy statement, and, if you agree with the terms, click I Accept and click Next.**

**Congratulations! You have completed the "Application Stage" for acquiring your digital certificate!**

## **AUTHENTICATION STAGE**

Digital Signature Trust (DST), the certification entity, will now begin the authentication process. Please be sure to send in your “Digital Certificate Agreement” (Page 8, Step 7a) as soon as possible. Expect a phone call from the CDX helpdesk to verify your applicant information. The authentication stage should take no longer than two business days.

You will receive an email acknowledging your application request. The email will provide an application ID and a website address that can be accessed to track your approval status.

- The email you receive will look like the page below.
- Please note that you will need your passphrase (Page 10f, Step 11) when the **Retrieval Stage** begins!!

Dear **Your Name**,

Thank you for applying with Digital Signature Trust (DST) for a TrustID certificate. We have received your application and have begun the approval and authentication process. As you know by now, your TrustID certificate stands for the highest level of authentication available, allowing you to use the Internet with confidence for your secure online transactions.

The approval process is normally completed within two business days of application submission. You can check the status of your application at any time by going to <http://www.trustdst.com/app-status.html>. You will need the following information in order to check your application process: Application ID , provided below, and your passphrase that you entered during your application process.

**Application ID: 662235**

Please remember to keep track of your passphrase. You must be able to provide your passphrase at the time you retrieve your certificate.

For any other questions, please contact DST Customer Support by sending e-mail to [helpdesk@identrus.com](mailto:helpdesk@identrus.com), or call 888-248-4447 (call direct at 801-326-5972). Customer Support representatives are available to assist you Monday through Friday, 7 a.m. to 6 p.m. Mountain Time.

Thank you again for applying for a TrustID certificate. We look forward to creating the highest level of trust in all of your digital transactions.

Sincerely,

Marlene Martinez  
Certificate Registration Manager  
Digital Signature Trust, LLC a subsidiary of Identrust, LLC.  
[www.trustDST.com](http://www.trustDST.com)

## **RETRIEVAL STAGE**

When your digital certificate is approved, you will receive an email from the CDX Helpdesk. This email provides you the website and activation code. If your email does not contain the activation code, it will include instructions on how to call the CDX Helpdesk to retrieve your activation code.

**Your Name,**

I have approved your digital certificate and now you will have to activate it, which will be the last part of creating your digital certificate. Please click the link below and follow the instructions to complete your application.

Thanks

Charles

-----  
This is a PRIVATE message. If you are not the intended recipient, please delete without copying and kindly advise us by e-mail of the mistake in delivery. NOTE: Regardless of content, this e-mail shall not operate to bind CSC to any order or other contract unless pursuant to explicit written agreement or government initiative expressly permitting the use of e-mail for such purpose.  
-----

Dear Administrator,

**Your Name** DST TrustSource Certificate request has been approved. Please have the client visit the following web address to retrieve the new certificate. He/She will be asked to use the following Activation Code and enter the passphrase he/she selected when submitting the request.

<http://www.digsigtrust.com/retrieve-cert.html>

**Activation Code: 1743737696**

Name: John Smith  
Account: 30353576-2  
E-Mail: John.Smith@email.com  
Cert Type: 520009  
Server: secure.digsigtrust.com

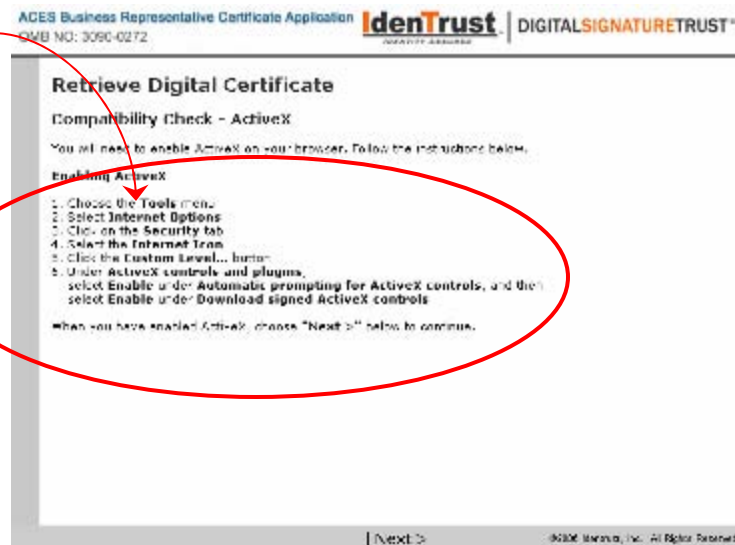
TrustSource Certification Service  
Digital Signature Trust Co.  
Salt Lake City, Utah  
trustsource@trustdst.com

**Step 13: From the previous email, click on or type in the Web site address to retrieve the digital certificate. Read and click Next.**



**Step 14: You will complete a compatibility check. You may be prompted to adjust certain security settings on your computer; these vary depending on your computer. Follow the onscreen instruction.**

- You may need to add <https://secure.digisigtrust.com> to your trusted sites



**Step 15: You now need your Activation Code (provided by email– see sample email on Page 13) and Passphrase (Page 11, Step 10f).**

ACES Business Representative Certificate Application **IdenTrust** | DIGITALSIGNATURETRUST™  
OMB NO: 3090-0272

---

### Retrieve Digital Certificate

**Login**

We have determined that your system is compatible. You may now begin the Retrieval Phase for your digital certificate.

To ensure that your digital certificate works properly, you need to complete the following steps just once. Following the steps and corresponding step-by-step instructions will ensure the successful retrieval and usage of your digital certificate.

To begin the Retrieval Phase, you must login by entering your activation code and passphrase you entered when you applied.

Activation Code:  [How do I get my activation code?](#)

Passphrase:  [I forgot my passphrase.](#)

| Next > ©2015 IdenTrust, Inc. All Rights Reserved.

**Step 16: Again, you will follow the instructions listed for the next few steps.**

ACES Business Representative Certificate Application **IdenTrust** | DIGITALSIGNATURETRUST™  
OMB NO: 3090-0272

---

### Retrieve Digital Certificate

**Key Pair Generation**

Keep the default selection below  
Microsoft Enhanced Cryptographic Provider v1.0

**Important:** On the next pop-up screen, please follow the Step-by-Step instructions to set your password.

**Step-by-Step Instructions:**

- Step 1. When the "Creating a new RSA exchange key" screen appears, choose "Set Security Level" and then choose "High" to enforce password protection, then click "Next >".
- Step 2. When the "Choose or create a password to protect this item" screen appears, choose "Create a new password for this item", then enter the password, then enter the password again to confirm it, then click "Finish".

| Next > ©2015 IdenTrust, Inc. All Rights Reserved.

## Step 17: If this warning screen appears, click Yes and continue

### Retrieve Digital Certificate

#### Key Pair Generation

Keep the default selection below

Microsoft Enhanced Cryptographic Provider v1.0

**Important:** On the next pop-up screen, please follow the Step-by-Step instructions to set your password.

#### Step-by-Step Instruction

Step 1. When the "Creating a new RSA exchange key!" screen appears, choose "Set Security Level" and then choose "High" to enforce password protection, then click "Next >"

Step 2. When the "Choose or create a password to protect this item" screen appears, choose "Create a new password for this item", then enter the password, then enter the password again to confirm it, then click "Finish"



## Step 17a: Click Set Security Level

### Retrieve Digital Certificate

#### Key Pair Generation

Keep the default selection below

Microsoft Enhanced Cryptographic Provider v1.0

**Important:** On the next pop-up screen, please follow the Step-by-Step instructions to set your password.

#### Step-by-Step Instructions:

Step 1. When the "Creating a new RSA exchange key!" screen appears, choose "Set Security Level" and then choose "High" to enforce password protection, then click "Next >"

Step 2. When the "Choose or create a password to protect this item" screen appears, choose "Create a new password for this item", then enter the password, then enter the password again to confirm it, then click "Finish"



| Next >

©2006 IdenTrust, Inc. All Rights Reserved.

## Step 17b: Choose High and then click Next

ACES Business Representative Certificate Application **IdeaTrust** | DIGITALSIGNATURETRUST™  
OMB NO: 3090-0272

### Retrieve Digital Certificate

#### Key Pair Generation

Keep the default selection below:  
Microsoft Enhanced Cryptographic Provider v1.0

**Important:** On the next pop-up screen, please follow the Step-by-Step instructions to set your password.

**Step-by-Step Instructions:**

Step 1. When the "Creating a new RSA exchange key" screen appears, choose "Set Security Level" and then choose "High" to enforce password protection, then click "Next >"

Step 2. When the "Choose or create a password to protect this item" screen appears, choose "Create a new password for this item", then enter the password, then enter the password again to confirm it, then click "Finish"

Next >

Creating a new RSA exchange key

Choose a security level appropriate for this item.

High  
Request my permission with a password when this item is to be used.

Medium  
Request my permission when this item is to be used.

Back Next Cancel

## Step 17c: Create a password for your exchange key, then click Finish

- An exchange key is a standard protocol used to ensure security for virtual private networks (VPN) and remote host or network access

ACES Business Representative Certificate Application **IdeaTrust** | DIGITALSIGNATURETRUST™  
OMB NO: 3090-0272

### Retrieve Digital Certificate

#### Key Pair Generation

Keep the default selection below:  
Microsoft Enhanced Cryptographic Provider v1.0

**Important:** On the next pop-up screen, please follow the Step-by-Step instructions to set your password.

**Step-by-Step Instructions:**

Step 1. When the "Creating a new RSA exchange key" screen appears, choose "Set Security Level" and then choose "High" to enforce password protection, then click "Next >"

Step 2. When the "Choose or create a password to protect this item" screen appears, choose "Create a new password for this item", then enter the password, then enter the password again to confirm it, then click "Finish"

Back Next Cancel

Creating a new RSA exchange key

Create a password to protect this item.

Create a new password for this item.

Password for: (C) IdeaTrust Private Key

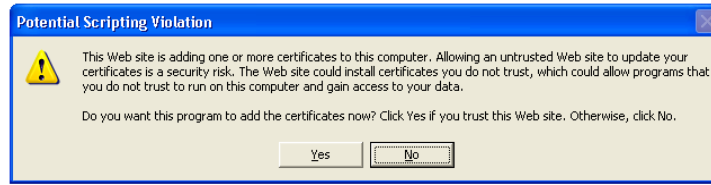
Password: .....

Confirm: .....

Back Finish Cancel

**PASSWORD CREATED!!**  
Remember it!!  
Keep It Secure!!

## Step 17d: Click Yes



## Step 18: Read the information and then click Next



## Step 19: Now the system wants to verify the certificate has been properly retrieved. Read the information on the screen, PRINT THE INSTRUCTIONS and click Next.



## **Step 20: Click on the appropriate digital certificate if you have more than one.**

CES Business Representative Certificate Application **IdenTrust** DIGITALSIGNATURETRUST™  
MB NO: 3090-0272

### Retrieve Digital Certificate

#### Instructions for Verifying Certificate Retrieval

Now that you have retrieved your certificate, follow these instructions to verify that it has been properly. These instructions will help you navigate through a series of windows. **Print these instructions** as you go through the process online.

1. Click "Next >". The **Client Authentication** window appears.
2. In the list, select the certificate you just retrieved, then click **OK**.
3. You may be prompted to provide your password. If prompted, provide the password for

In the event that the certificate cannot be verified, due to selecting the wrong certificate, or clicking instead of **OK** at the **Client Authentication** window, close any browser windows that are open, browser and return to the following URL to begin the verification process again:

<https://secure.digitalsignaturetrust.com/tsapp/retrieve-verify-instr.jsp?AT=009&CT=52000>

If the **Congratulations** page appears, your certificate has been successfully retrieved and download process is complete.



| Next > ©2005 IdenTrust, Inc. All Rights Reserved

## **Step 21: This congratulations screen assures you have successfully retrieved your certificate. Click Yes and the process is complete.**

- If this screen does not appear, look at the instructions that you printed in Step 20 or call the CDX Helpdesk.

ACES Business Representative Certificate Application **IdenTrust** DIGITALSIGNATURETRUST™  
OMB NO: 3090-0272

### Congratulations, Certificate Retrieval Completed Successfully

We have verified that your certificate has been successfully downloaded.  
It is available on your system and ready for use.



| Finish > ©2005 IdenTrust, Inc. All Rights Reserved

### III. Downloading/Exporting your Digital Certificate

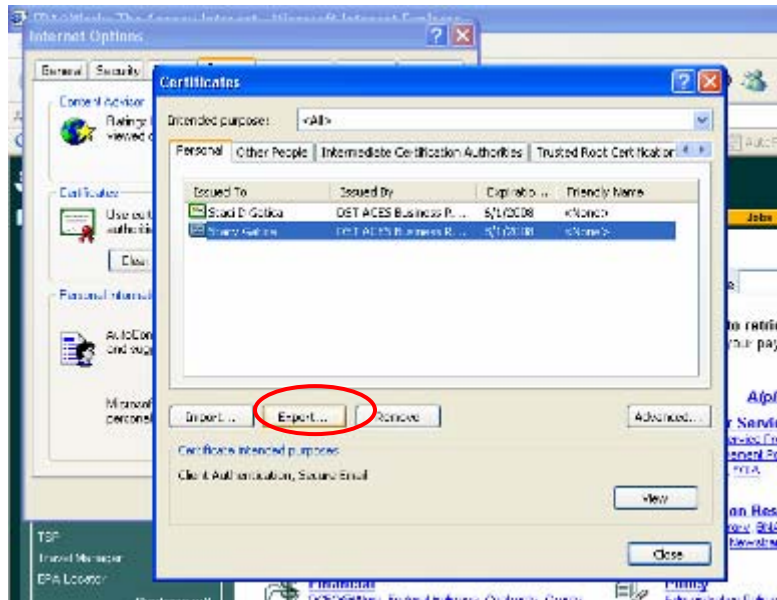
- You must export your certificate and place it onto your PC. This will allow your PC to be identified when you submit your data through CDX. In simple terms, this process is providing your computer with the ability to sign digital forms you will be submitting to EPA.

The following is a technical note, and could be helpful if you need IT support:

- This procedure enables the applet to access the user's digital certificate in a platform independent fashion. Since browsers (e.g., Microsoft Internet Explorer, or Firefox) manage certificates in different ways, the applet has no access to the customer's certificate. This procedure provides a way around this problem, by creating a "copy" of the user's certificate (from their browser) into a secure "keystore" file on their computer.
- The certificate export procedure is a mechanism to copy a user's certificate (from their browser's proprietary keystore) into standard keystore file (NIST approved PKCS#12 format) on their PC file system.

**Step 22: From the Internet, click the Tools menu and select Internet Options. Click the Contents tab and then click the Certificates button near the center of the dialog box. You should see your certificate(s) in the dialog box that appears.**

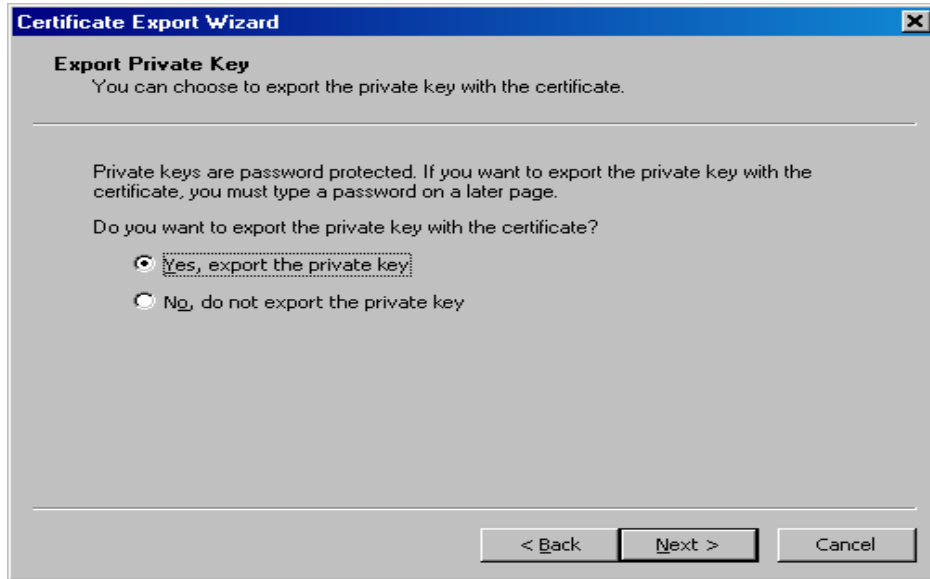
- Select the certificate you wish to export and click the **Export** button.



**Step 23: The Certificate Export Wizard appears. Read the page and click Next.**

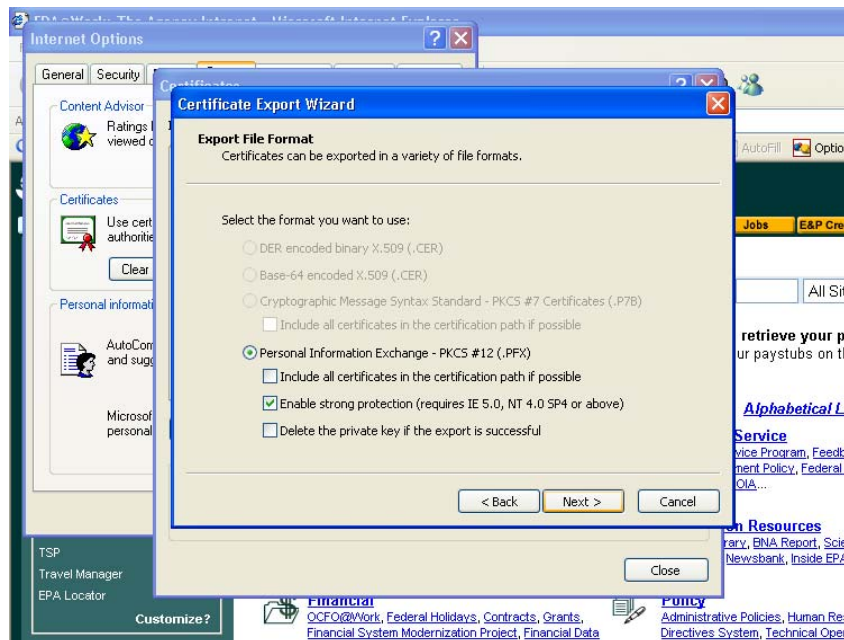


**Step 23a: Select the “Yes, export the private key” option and then click Next.**



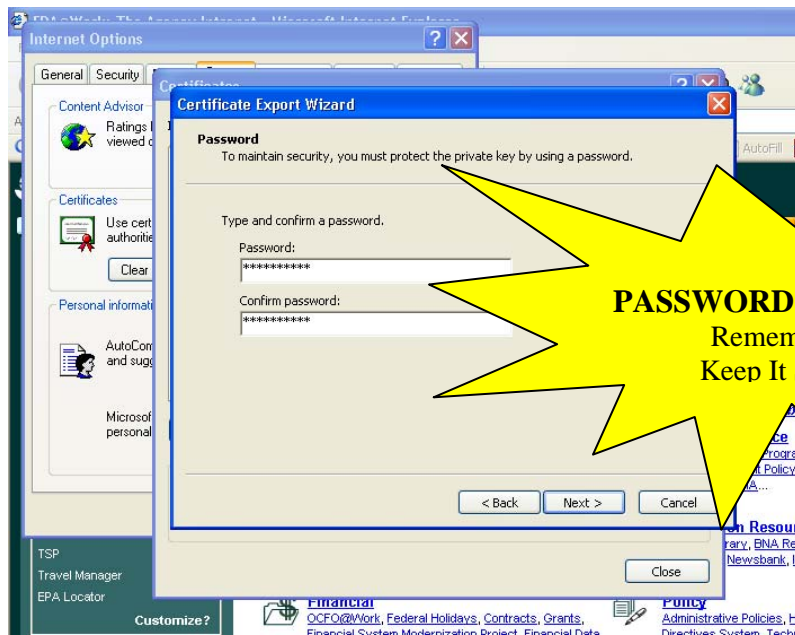
**Step 23b: Select the “Personal Information Exchange – PKCS #12 (.PFX)” format, and check the middle option (Enable strong protection).**

- **Do not select** “Delete the private key if the export is successful”
- Click **Next** to continue.



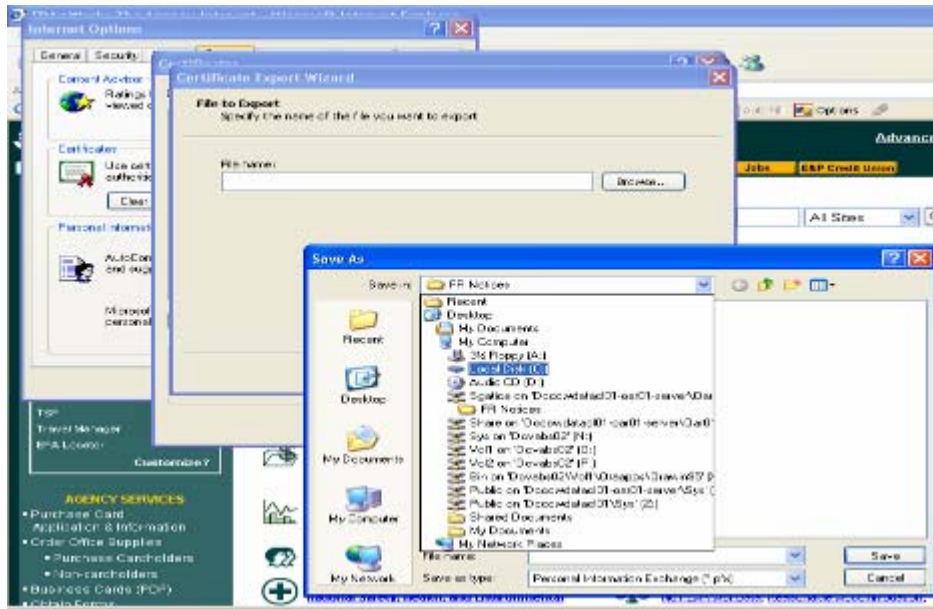
**Step 23c: Type a password for your new keystore. This password does not have to be the same as the password for your certificate, CDX account, nor your computer. In fact, it is wise to have a DIFFERENT password for the keystore.**

- Click **Next** when done.
- A keystore is a protected database that holds your certificates and keys.



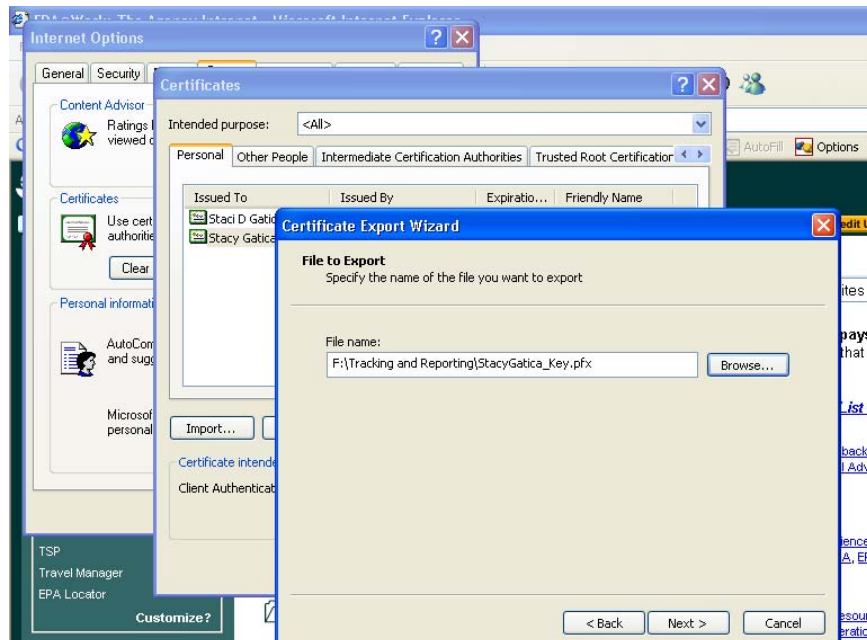
**Step 24: Another screen appears asking you the “File to Export.” Click Browse.**

**Step 24a: Navigate to the directory where you want to save your keystore file**



**Step 24b: Specify a file name for your keystore. Note: the export format should use the “Personal Information Exchange(pfx)” automatically.**

- Click Next.



**Step 24c: Click Finish to close the wizard**



**Step 25: You may see the following confirmation dialog box. If so, click OK.**



**Step 26: Enter your password (from Step 23c) for the export process. EPA suggests NOT checking the "Remember password" box. Click OK.**

**Step 27: Click OK to recognize the export was successful! You have completed Part 1 of the Electronic Reporting Guidance!!**

