

Drug Enforcement Administration

Controlled Substance Ordering System

Subscriber Manual

Version 3.0
July 29, 2024



Table of Contents

1.0	CSOS Overview.....	1
1.1	CSOS Certificates	1
1.2	CSOS Subscriber Roles	2
1.3	Basic Overview.....	3
2.0	CSOS Enrollment.....	4
2.1	Creating an Account.....	5
2.2	Helpful Links.....	13
2.3	Initial Login	14
2.4	The Dashboard.....	15
2.5	Create an Enrollment Request.....	16
2.5.1	RA Process.....	19
2.5.2	Certificate Issuance	19
3.0	Certificate Retrieval.....	20
3.1	Subscriber Certificate Retrieval Instructions.....	21
3.1.1	Policy Agreement	21
3.1.2	Trust Setup.....	21
3.1.3	Website Login	22
3.1.4	DEA E-Commerce CA Certificate	25
3.2	Certificate Denial.....	33
4.0	Other Website Actions.....	34
4.1	My Information Tab	34
4.1.1	Current DEA Registrations	34
4.1.2	Renew	35
4.1.3	Revoke	36
4.1.4	Validation Troubleshooting.....	37
4.2	Registrants and Coordinators Tab.....	39
4.2.1	Member Approvals	39
4.2.2	Member Revocations.....	41
4.2.3	Status of Requests.....	42
4.2.4	Password Reset.....	42
5.0	Certificate Management.....	48
5.1	Certificate Renewal	48
5.2	Certificate Revocation.....	49
5.2.1	Revocation Reasons	49
5.2.2	Procedure for Revocation Requests.....	50
5.3	Certificate Information.....	51
5.3.1	View/Open the certificate	51
5.3.2	DEA Certificate Version Number Information	51
5.3.3	DEA Registrant Name	53
5.3.4	DEA Schedules.....	54
5.3.5	Convert a Hexadecimal to Binary	55
5.3.6	DEA Business Activity	57
5.3.7	DEA Postal Address.....	59
5.3.8	DEA Registration Number	60
6.0	Certificate Security.....	62
6.1	Private keys must be kept private.	62
6.2	Secure access to the private key.....	62
6.3	Enable the Workstation/PC Inactivity Timeout for 10 minutes.	63
6.4	Anti-Virus/Spyware Software	63

6.5	Backing-up or Escrowing the Private Key	63
6.6	Method of Deactivating Private Key	63
6.7	CSOS Application and Auditing Information	63
7.0	CSOS Software Application Audit Requirements.....	64
8.0	Contact Information	65
8.1	Support Center Contact Information	65
A.0	Glossary	66
B.0	Acronyms	67
C.0	Registrant Attestation.....	68
D.0	Registrant Agreement.....	69
D.1	Organization Contact for CSOS Registration Authority.....	69
D.2	Distribution of Authorization Codes.....	69
D.3	Certificate Revocation.....	69
E.0	Subscriber Agreement.....	70
E.1	Terms of Agreement.....	70
E.1.1	Representations.....	70
E.2	Subscriber Enrollment Procedures	70
E.3	Identification Information Attestation.....	70
E.4	Obligations.....	71
E.4.1	Certificate Review	71
E.4.2	Certificate Protection.....	71
E.5	Acceptable Use	71
E.6	Subscriber Account Management	71
E.7	Certificate Expiration	71
E.8	Terms of Agreement.....	71
E.8.1	General.....	71
E.8.2	Availability	72
E.8.3	Requests.....	72
E.8.4	Dispute Resolution and Governing Law	72
E.8.5	Extraordinary Events	72
E.8.6	Privacy Notification.....	72
E.8.7	Additional Resources.....	72

1.0 CSOS Overview

The Drug Enforcement Administration (DEA) Controlled Substance Ordering System (CSOS) allows for secure electronic transmission of controlled substance orders without the supporting paper Form 222. The adoption of CSOS standards is the only allowance for electronically signing and transmitting orders for Schedule I (CI) and II (CII) controlled substances.

Each individual requesting the ability to sign electronic orders for controlled substances must enroll with DEA. This Subscriber Manual documents enrollment with DEA in the CSOS program as well as assistance with certificate acquisition and management. Once a CSOS subscriber has enrolled with DEA and obtained his/her digital certificate(s), he/she may place electronic orders of controlled substances from participating suppliers/wholesalers using CSOS approved ordering software.

1.1 CSOS Certificates

CSOS Signing Certificates contain unique information identifying and linking an individual registrant with a DEA registration. Signing Certificates authorize registrants to sign orders for any controlled substances for which they have registered with the DEA.

Each individual requesting the ability to sign electronic CI and CII controlled substance orders must obtain his/her own CSOS Signing Certificate. **Each Signing Certificate is specific to one DEA Registration number for one individual.**

Multiple Signing Certificates must be requested for applicants requiring the ability to sign electronic CI and CII controlled substance orders for multiple DEA Registration numbers.

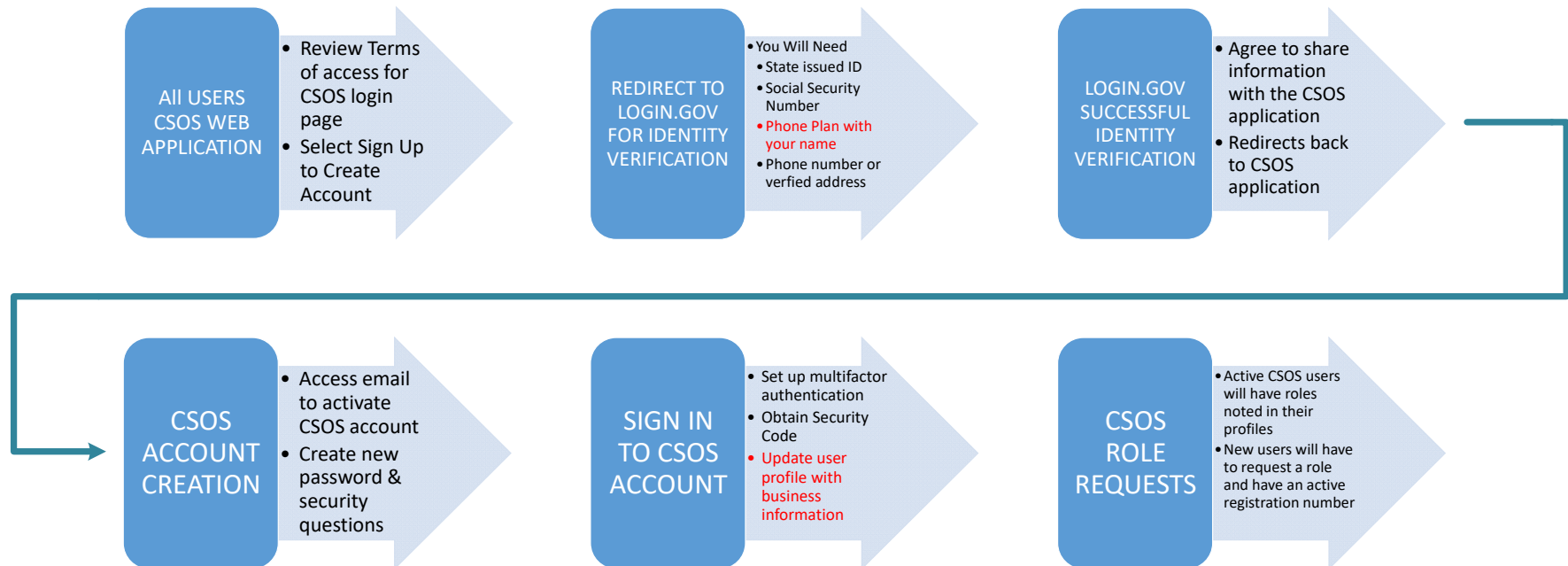
1.2 CSOS Subscriber Roles

This Subscriber Manual contains enrollment instructions in Sections 2 and 3, specific to each subscriber role.

CSOS Role	First Registrant	Registrant	Admin Coordinator	Coordinator	Power of Attorney
Description:	The First Registrant is the primary individual who signed the most recent DEA registration application or renewal application, or a person authorized to sign a registration application (must be the first requested role)	A DEA Registrant is the individual who signed the most recent DEA registration application or renewal application, or a person authorized to sign a registration application	Individual designated to serve as the DEA Registrant's CSOS coordinator and point of contact regarding issuance of, revocation of, and changes to digital certificates. The Admin Coordinator does not receive CSOS certificates.	Individual designated to serve as the DEA Registrant's CSOS coordinator and point of contact regarding issuance of, revocation of, and changes to digital certificates issued under the Registrant's registration	A DEA Registrant may grant another individual the power of attorney to sign controlled substance orders on the Registrant's behalf
Required role?	Yes	No	No	Yes	No
Authorized by:	DEA Registration Authority (RA) Team. Please see section 2.5.1.	First Registrant for the requested DEA Registration number(s)	First Registrant for the requested DEA Registration number(s)	Registrant or Coordinator for the requested DEA Registration number(s)	Registrant for the requested DEA Registration number(s)

1.3 Basic Overview

Below is a high-level diagram, giving a basic overview of the process:



2.0 CSOS Enrollment

All users, regardless of whether the applicant currently holds a CSOS certificate, must create an account in the Controlled Substance Ordering System (CSOS) the first time the site is accessed.

This section provides high level activities that describe the Registrant enrollment Request process is designed to walk you (the registrant) through creating your first enrollment request. This includes:

- Creating Login.gov and CSOS accounts
- Logging into CSOS for the first time
- A brief overview of the Dashboard
- Requesting your First Registrant enrollment request
- A brief overview of the RA and CA approval processes

Note that all applicants will be redirected to Login.gov when logging into the CSOS Web Application for the first time.

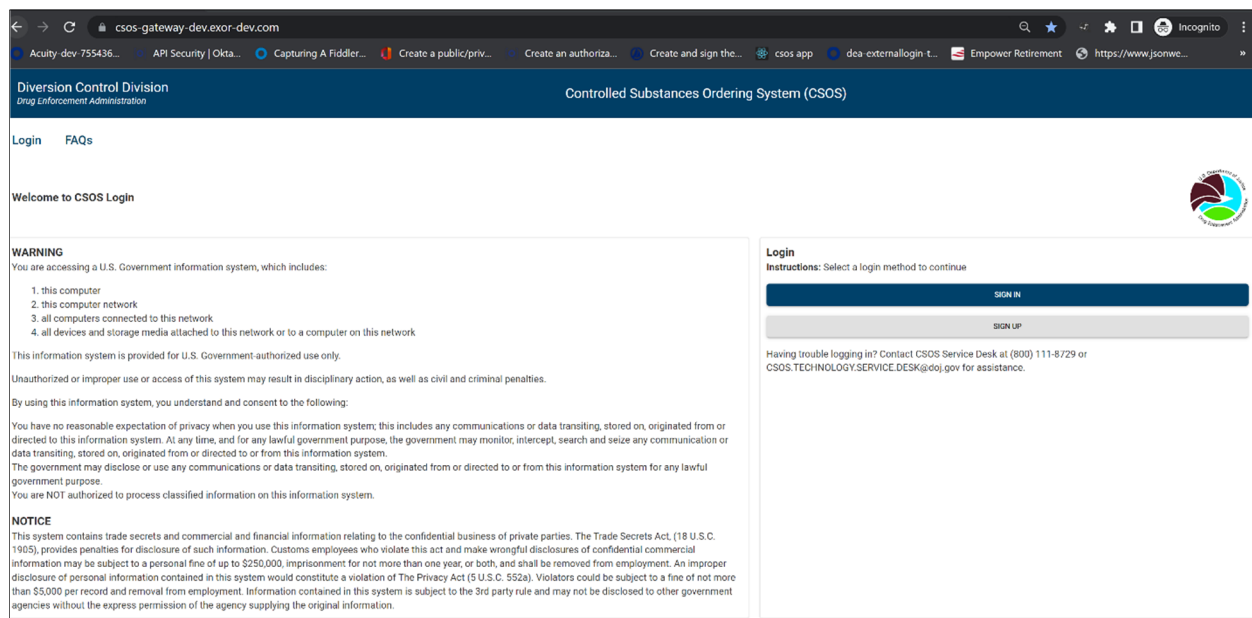


Figure 1: CSOS Home screen

From this screen, several actions are possible:

- Sign up for a new CSOS account
- Login to an existing CSOS account
- View the CSOS Frequently Asked Questions (FAQ) page

By using the CSOS Web Application, you must explicitly agree to the following:

- Registrant attestation (see Appendix C)
- Registrant Agreement (see Appendix D)
- Subscriber Agreement (see Appendix E)

The above documents will be downloaded when creating any enrollment request.

2.1 Creating an Account

1. Click the **Sign Up** button to begin the account creation process. This is the found on the right side of the Home screen.

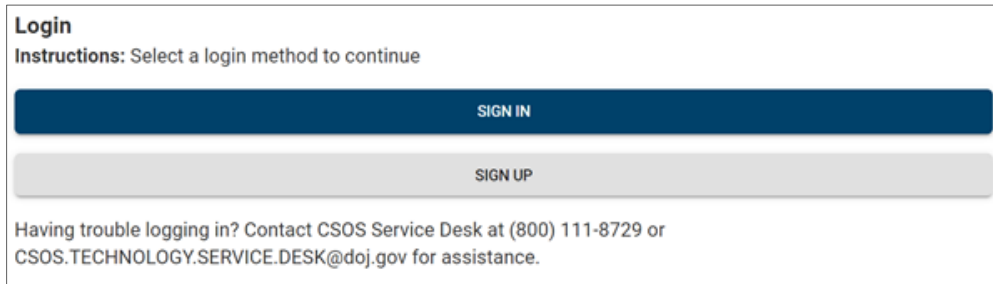


Figure 2: CSOS Sign In/Sign Up Buttons

2. CSOS will display log in instructions. Once you have read them, click the **Sign Up** button to continue.



Figure 3: Sign Up Instructions

3. You will be directed to Login.gov where you will be asked to sign in or Create an account.

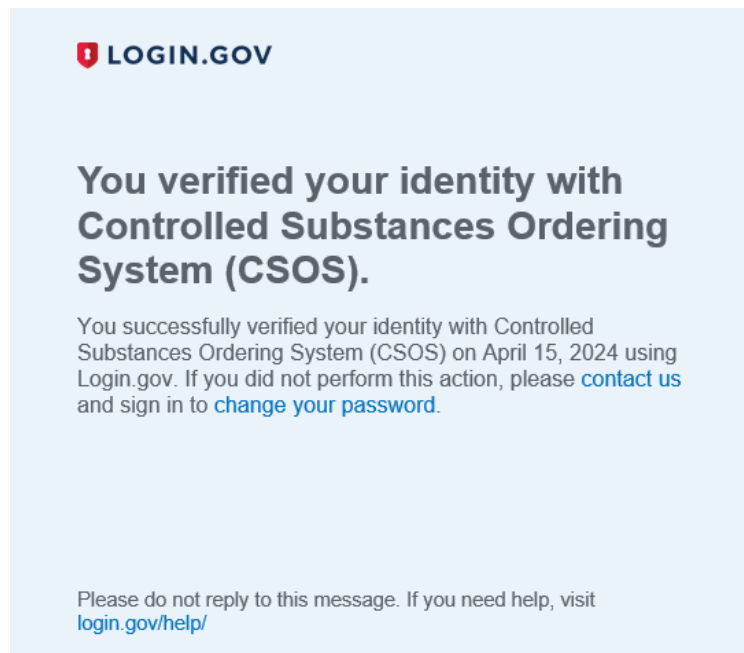
Note that if there are any problems creating an account in Login.gov, then Login.gov must be contacted for additional support.

Figure 4: Login.gov Sign In

At this point you must create a Login.gov account. Should you need additional assistance during this process, please refer to the Login.gov Help center at <https://login.gov/help>.

4. Once Login.gov has been able to verify your identity you will be directed back to the CSOS web application. Click the **OK** button to continue. An email will be sent to the email address you registered previously.

You will receive an email similar to the following, confirming that your identity has been verified.



5.

6. Figure 5: Identity Verified Email

7. Click the **OK** button to continue.

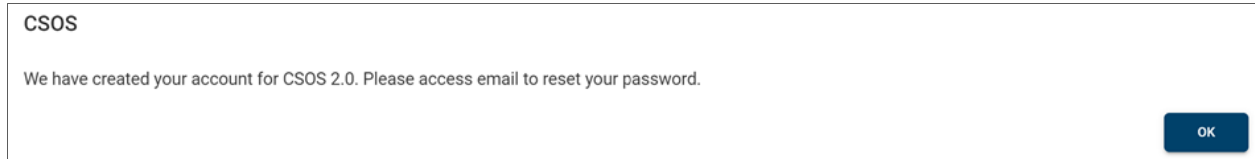


Figure 6: CSOS Account Created

8. Click the **Activate Drug Enforcement Administration Account** button to continue.

Note that the button and link in the email will expire after 7 days. You will need to contact the Helpdesk if the button and link has expired.

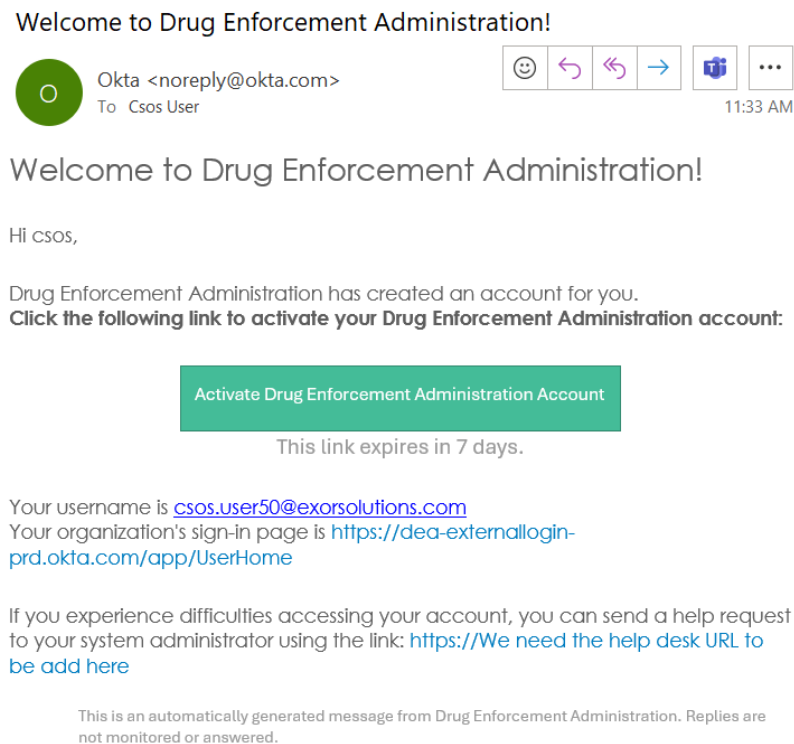


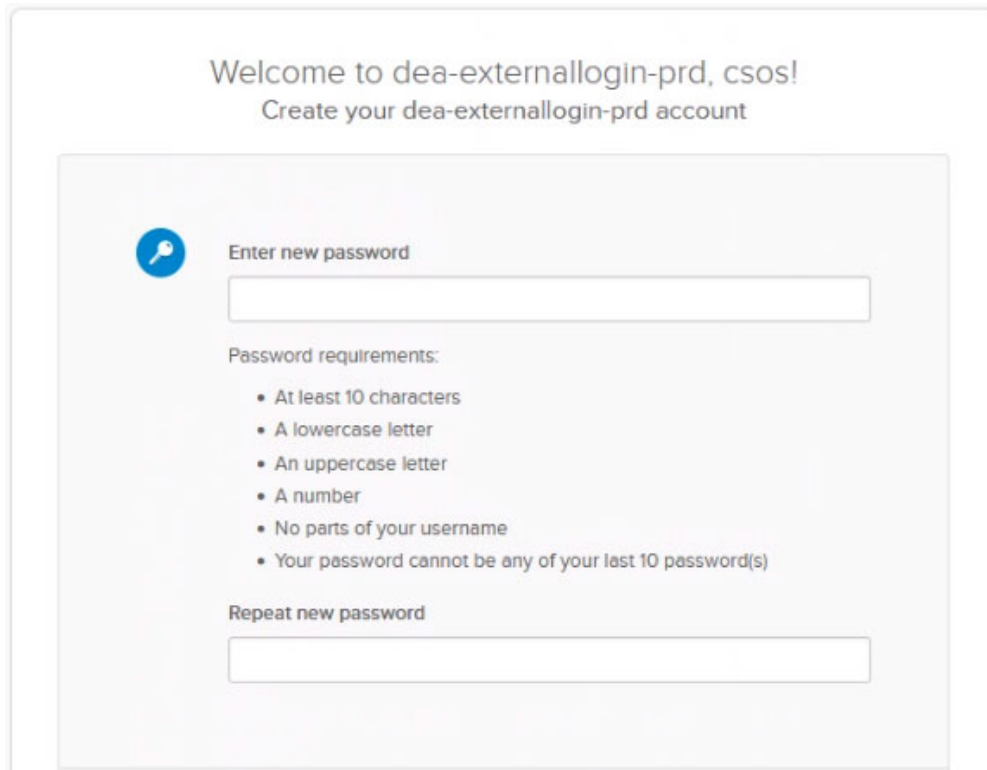
Figure 7: Welcome Email

As this is the first time logging in, CSOS will require you to reset your password. An email will be sent to the email address you entered during your account creation. Your username is printed in the grey box in the email.

9. CSOS will require you to create a new password.

Note, this is not the same password that was created in Login.gov. You are now creating a new password specifically for CSOS.

10. Click the **Reset Password** button to continue.



The screenshot shows a web form titled "Welcome to dea-externallogin-prd, csos! Create your dea-externallogin-prd account". The form contains a blue circular icon with a white person silhouette. Below the icon is the text "Enter new password" followed by a text input field. Underneath is the heading "Password requirements:" followed by a bulleted list: "At least 10 characters", "A lowercase letter", "An uppercase letter", "A number", "No parts of your username", and "Your password cannot be any of your last 10 password(s)". Below the list is the text "Repeat new password" followed by another text input field.

Figure 8: Password Reset

11. Click the **Send me the code** button to have CSOS send a text message to your email address.

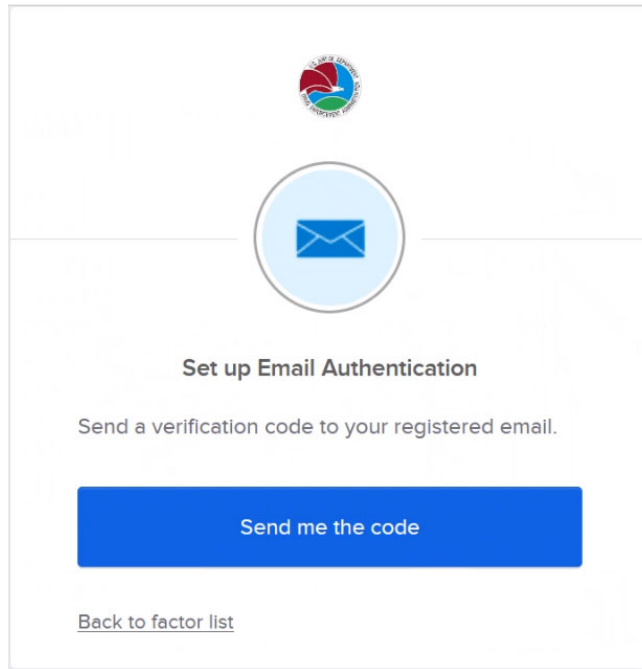


Figure 9: Send Authentication Code

You will receive an email from CSOS with the subject line: "Action Required: Confirm your email address." The email will contain a verification code.

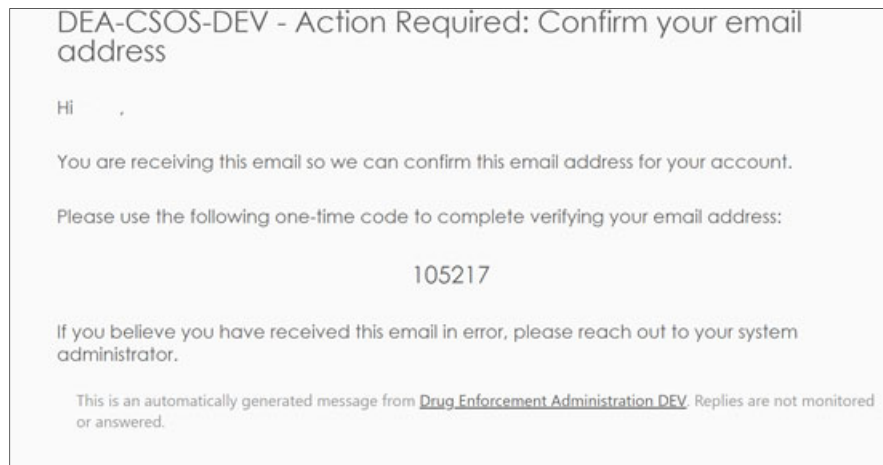


Figure 10: Verification Code Email

39. Enter the verification code you received in the email

The screenshot shows a web interface for setting up email authentication. At the top center is a circular logo with a colorful design. Below it is a large blue circle containing a white envelope icon. The main heading is "Set up Email Authentication". Below the heading, a message states: "A verification code was sent to c...0@exorsolutions.com. Check your email and enter the code below." Underneath this message is a label "Verification code" followed by a rectangular input field. Below the input field is a prominent blue button with the text "Verify". At the bottom left of the form area, there is a link labeled "Back to factor list".

Figure 11: Enter Verification Code

After you reset your password, you will be prompted to set up MFA through Okta.

40. Select a form of MFA, and follow the onscreen prompts.



Set up multifactor authentication

Your company requires multifactor authentication to add an additional layer of security when signing in to your Okta account



Okta Verify

Enter single-use code from the mobile app.

[Setup](#)



Google Authenticator

Enter single-use code from the mobile app.

[Setup](#)



Email Authentication

Enter a verification code sent to your email.

[Setup](#)

Figure 12: MFA Selection

Okta will send an automated email (similar to one show below) confirming that MFA has been set up properly.

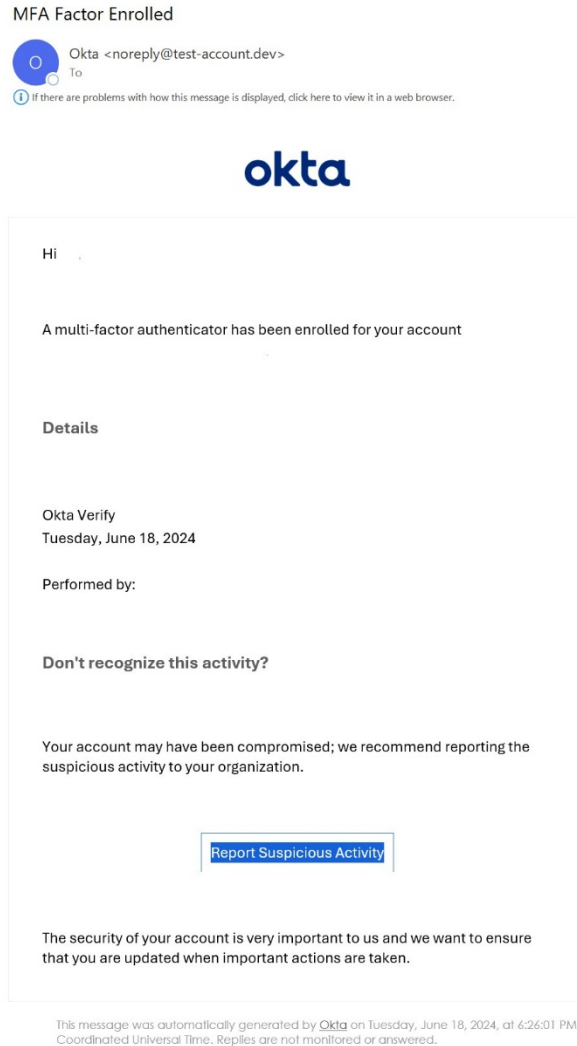


Figure 13: MFA Confirmation

2.2 Helpful Links

At any time while signing in, you can click the **Need Help Signing In** link to bring you to the *Sign-in Help* page.

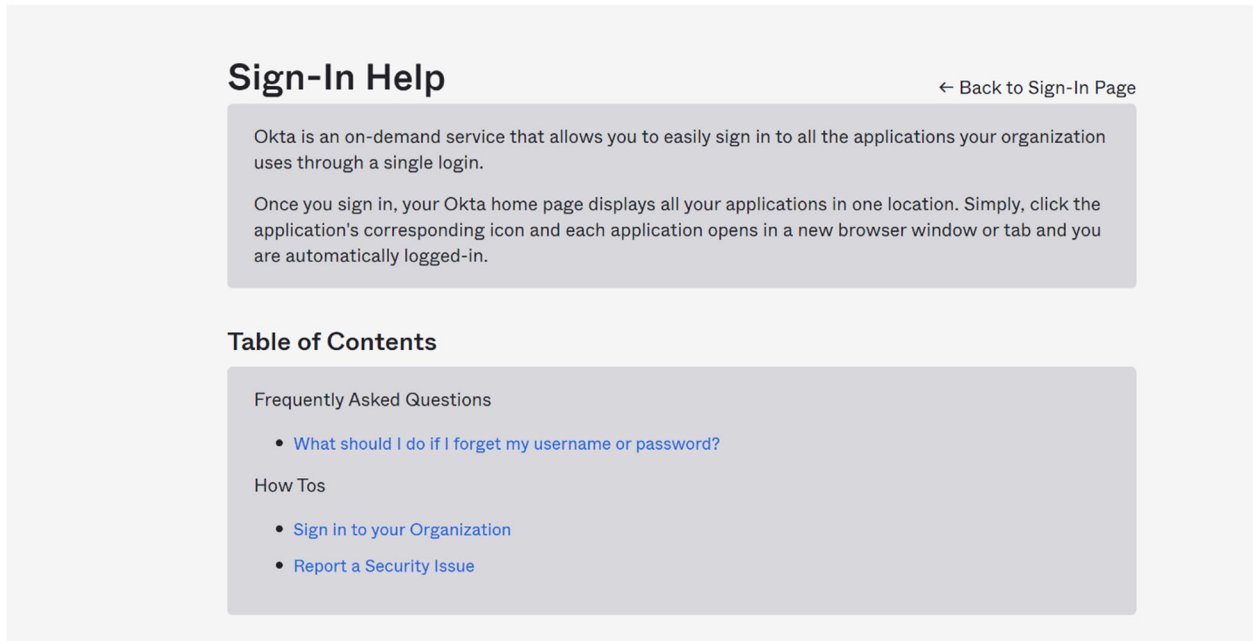
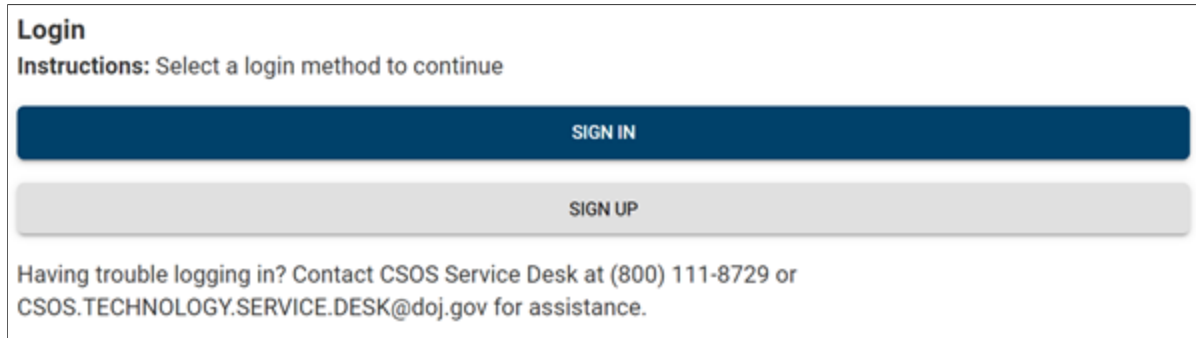


Figure 14: Sign-in Help

2.3 Initial Login

Login.gov will now return you to the CSOS Web Application, where you will proceed to log in for the first time. You must first create a user profile, entering your phone and address information, before progressing further.

1. Now that you have created a Login.gov account, click the **Sign In** button.



The screenshot shows a login interface with the following elements:

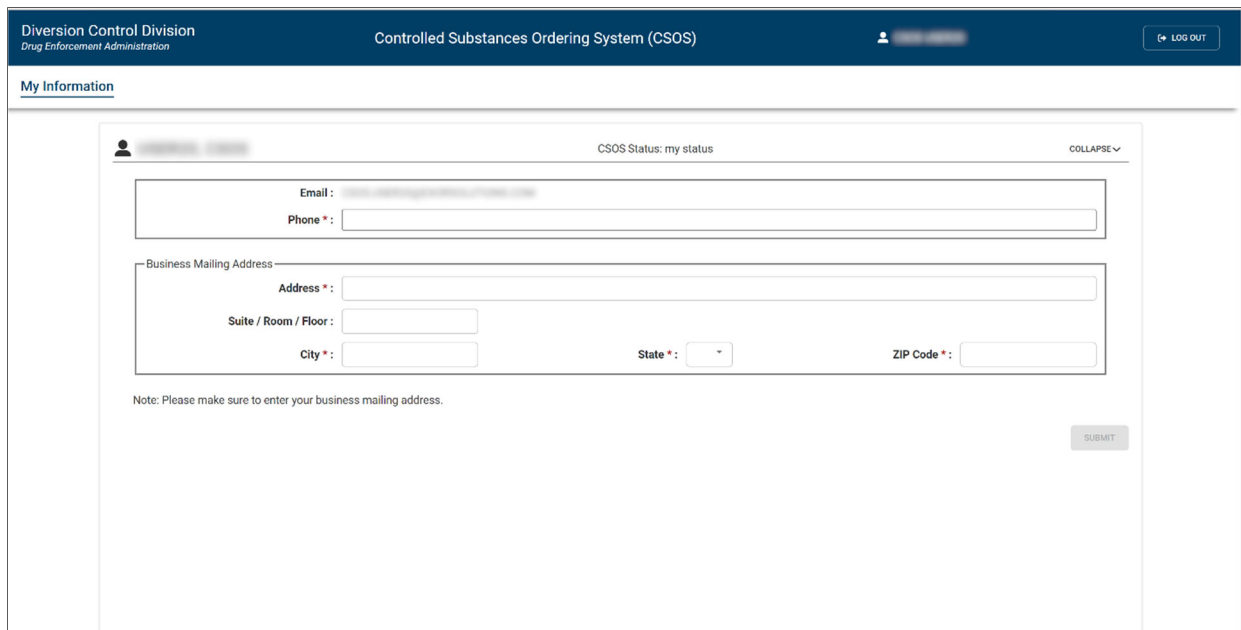
- Login** header
- Instructions:** Select a login method to continue
- A dark blue button labeled **SIGN IN**
- A light gray button labeled **SIGN UP**
- Text: Having trouble logging in? Contact CSOS Service Desk at (800) 111-8729 or CSOS.TECHNOLOGY.SERVICE.DESK@doj.gov for assistance.

Figure 15: Login

2. Follow the onscreen prompts to complete your initial login.

CSOS will require that you enter your business **Phone** and **Address** information.

3. Click the **Submit** button.



The screenshot shows the 'My Information' page in the CSOS system. The page header includes 'Diversion Control Division Drug Enforcement Administration' and 'Controlled Substances Ordering System (CSOS)'. A 'LOG OUT' button is visible in the top right corner. The main content area is titled 'My Information' and contains a form with the following fields:

- Email:** [Text input field]
- Phone *:** [Text input field]
- Business Mailing Address:**
 - Address *:** [Text input field]
 - Suite / Room / Floor:** [Text input field]
 - City *:** [Text input field]
 - State *:** [Dropdown menu]
 - ZIP Code *:** [Text input field]

A note at the bottom of the form reads: 'Note: Please make sure to enter your business mailing address.' A 'SUBMIT' button is located at the bottom right of the form area.

Figure 16: My Information

Your profile will be updated.



Figure 17: User Profile Updated

If you previously subscribed with a paper form, then your information will be imported over to your new CSOS account.

If your information has not been migrated, contact the CSOS Helpdesk for further assistance.

2.4 The Dashboard

The **Dashboard** is the central interface from which you will create and track CSOS requests. It is divided into two primary sections:

- **My Information**
- **My Team Members**

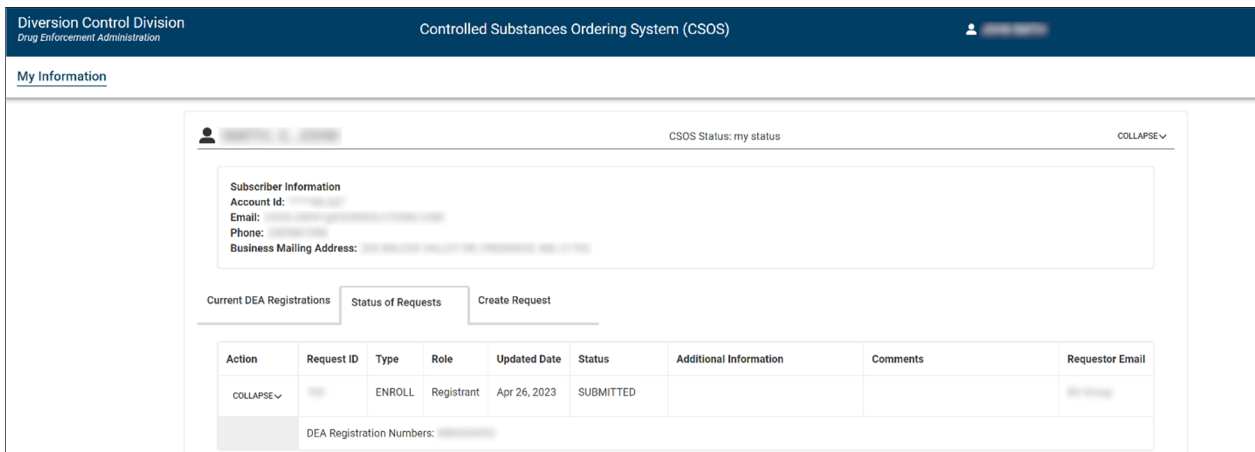


Figure 18: My Information Dashboard

2.5 Create an Enrollment Request

*Note that this must be completed for first time subscribers. No other action may be taken until the **First Registrant** has enrolled into CSOS.*

*If you are a current CSOS subscriber, or have previously registered with CSOS using a paper application, click on the **Current DEA Registrations** tab to verify your available DEA registrations (see 4.1.1: Current DEA Registrations for more information).*

Perform the following steps to create an Enrollment request:

Figure 19: Create Registrant Enrollment Request

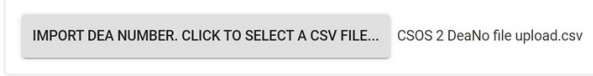
1. Select the **Create Request** tab.
2. Select **Enroll** from the *Request Type* menu.
3. Select **Registrant, Principal Coordinator, Alternate Coordinator, or Power of Attorney** from the *Role* menu.
 - a. *Note that selecting another role without a Registrant previously approved will return an error.*
4. Indicate whether this registrant will fulfill the role of CSOS Principal Coordinator.
 - a. *Note that the Power of Attorney role may not be a Principal Coordinator.*
5. Add any additional comments relevant to the created request in the *Comments* field.

Figure 20: Enter DEA Numbers

6. Add one or more DEA numbers.
 - a. If you wish to manually add a DEA number, select the **Add DEA Number** radio button.

- i. Enter a valid DEA number in the **DEA Registration #** field.

- ii. Click the **Add** button.
- b. If you wish to import a DEA number from a CSV file, select the **Import File** radio button.



- i. Click the **Import DEA Number. Click to Select a CSV File** button to import a CSV file.

```
DL - Notepad
File Edit Format View Help
document:
  type: license
  first_name:
  last_name:
  middle_name:
  address1:
  address2:
  city:
  state:
  zipcode:
  dob:
  phone:
  state_id_number:
  state_id_type: drivers_license
  state_id_jurisdiction:
```

Figure 21: Sample CSV File

- c. If you wish to select one or more DEA numbers from a list, click the **Select from List** radio button. Complete the following steps:

Add DEA Registration Number ↓

DEA Number Selection Options ⓘ :

Add DEA Number
 Import File
 Select from List

Chaincode Business
 TaxId
 City
 State
 - OR -
 ZIP Code ⓘ

SEARCH CLEAR

Available DEA Registration Numbers to Request Filter

Rows per page: 10 1-1 of 1 < >

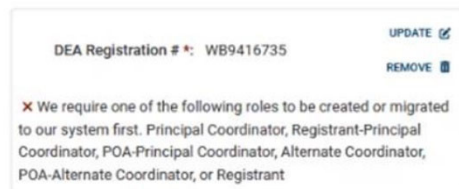
<input type="checkbox"/>	DEA #	Name	Address	City	State	Zip
<input checked="" type="checkbox"/>						

Rows per page: 10 1-1 of 1 < >

ADD

Status: NEW ✓

- i. Check the checkbox if you are part of a retail chain. If you are not, leave this box unchecked.
 - ii. Select one of the following from the drop-down menu: Tax ID, SSN, National Provider Identification (NPI), or DEA Number.
 - iii. Enter a valid tax ID number, SSN, NPI, or DEA Number. Optionally, you may also enter a City, State, or Zip code.
 - iv. Click the **Search** button.
 - v. Check one or more of the DEA numbers that appear in the list.
 - vi. Click the **Add** button.
7. Click the **Validate and Save** button to validate the added DEA number(s).
 - a. If the DEA Number does not pass validation, this will be reported. Consult the Validation Troubleshooting table (section 4.1.4) to resolve the issue.
8. Added DEA numbers will be listed with:



- a. Options to **Update** and **Remove** the DEA number
 - b. If necessary, a warning validation error.
9. Click the **Submit** button.
10. You must read through, agree to, and download the following CSOS agreements in order to proceed:

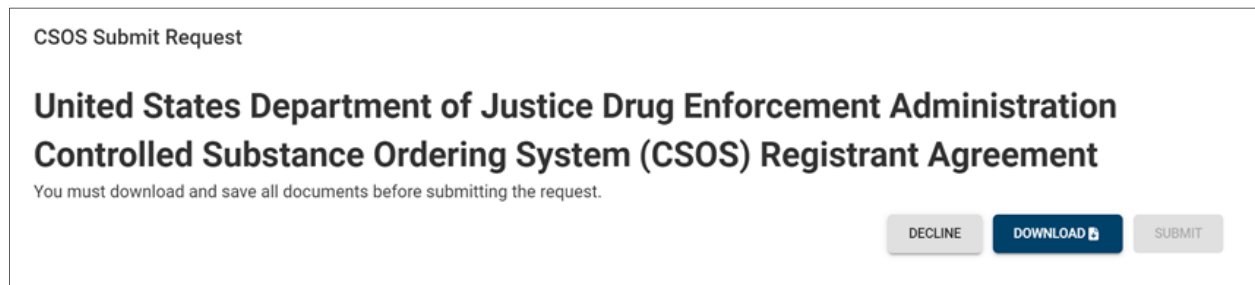


Figure 22: Download CSOS Agreements

- Registrant Attestation
- Registrant Agreement
- Subscriber Agreement

11. After downloading all of the CSOS agreements, click the **Submit** button.

2.5.1 RA Process

Note that this section is provided for information purposes. No direct action is expected from the subscriber.

Note that the Registration Authority (RA) will only approve the First Registrant enrollment. All other roles will be approved by the First Registrant.

Once the RA receives the First Registrant request, the RA verifies that they are a DEA registrant. After verification is obtained, the First Registrant is enrolled in CSOS.

2.5.2 Certificate Issuance

Once enrollment is complete, DEA sends the applicant one E-mail and one postal mailed document for each CSOS Certificate issued. These Activation Notices are to be used *by the applicant* for retrieving his/her CSOS Certificate(s) via DEA's secure certificate retrieval Web page.


For each CSOS Certificate issued:


- An **Access Code** is sent to the applicant via E-mail from regauth@DEAecom.gov to the E-mail address provided on the application
- An **Access Code Password**, a Web site address for Certificate retrieval, and Web site log in information, is sent via postal mail to the Coordinator, whose address was provided on the Coordinator application. The Principal Coordinator must forward the *unopened* mailed document to the Registrant.


After receiving the retrieval information, the *subscriber (certificate owner)* accesses DEA's secure certificate retrieval Web site to retrieve his/her CSOS Certificate(s). Instructions for retrieving CSOS Certificates are provided in Section 0 of this Subscriber Manual.


3.0 Certificate Retrieval

Retrieving and installing a CSOS Certificate creates the digital certificate and stores it in the browser. This certificate may remain in the browser until ordering software is installed on the computer.

 Activate CSOS Certificates on the computer that will be used for electronic ordering of controlled substances. Certificates may be transferred to other computers. To place an electronic order, the certificate will need to be present on the ordering computer.

 Only the owner of the certificate may retrieve it.

 Certificates may only be retrieved once.

 Do not disclose the Certificate's password to anyone.

This section discusses the technical requirements and processes for retrieving a CSOS digital certificate. Certificates may be retrieved once the applicant has received an Email and a mailed activation notice for the Certificate. One Email and postal mail document pair will be sent for each Certificate.

1. CSOS Signing Certificate activation notices contain a DEA Registration number. The Email and postal mail document should be matched based on the certificate owner's name and the DEA Registration number.

3.1 Subscriber Certificate Retrieval Instructions

3.1.1 Policy Agreement

The owner of the certificate is required to review the following policy information, and click **I Accept** to indicate that he/she understands and agrees to comply with the stated policy.

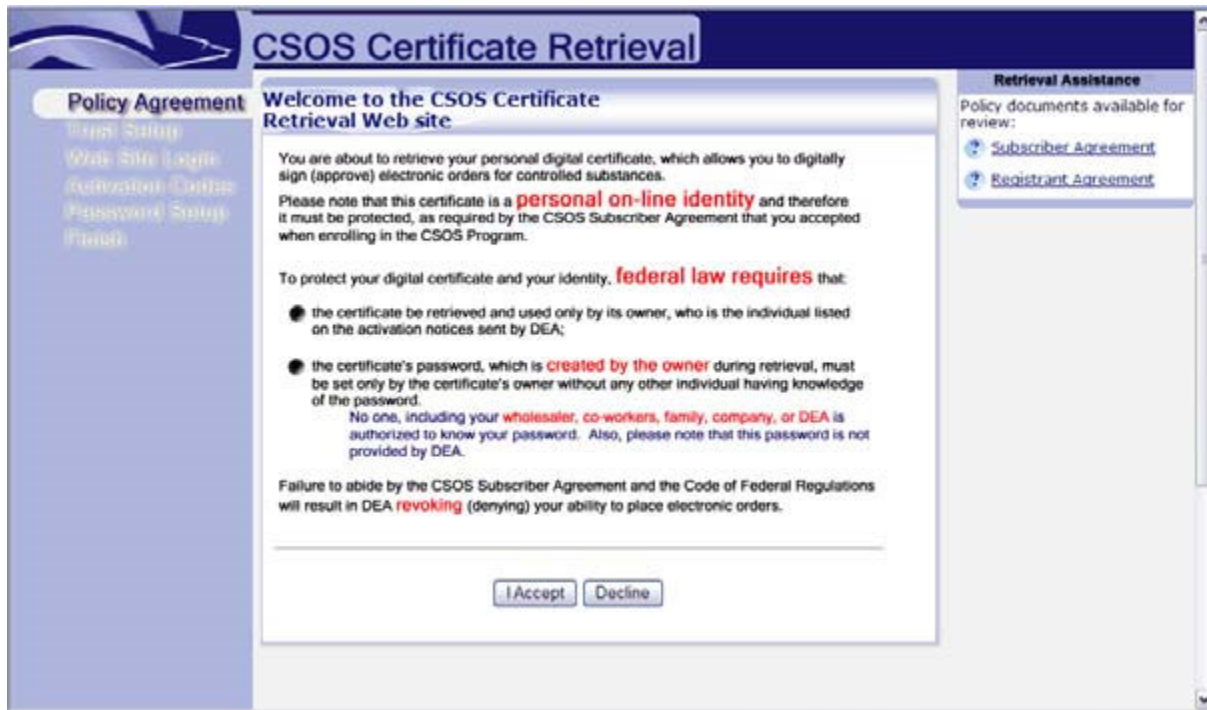


Figure 23: Policy Agreement

3.1.2 Trust Setup

DEA's Certification Authority (CA) has three CA Certificates:

- Root CA 1 Certificate: [Install the CSOS Root CA](#)
- Sub CA 1 Certificate: [Install the CSOS Sub CA 1](#)
- Sub CS 2 Certificate: [Install the CSOS Sub CA 2](#)

Install the Root CA 1, as well as Sub CA 1 and Sub CA 2 certificates as documented on the side panel of the Web page and in the following steps. These CA certificate installations are required once per ordering computer. If you are unsure whether the certificates have been installed, you may do so again, since there is no harm in installing the CA certificates multiple times.

When finished, click the **Click to continue after installing all DEA CA Certificate** button at the bottom of the screen.

3.1.3 Website Login

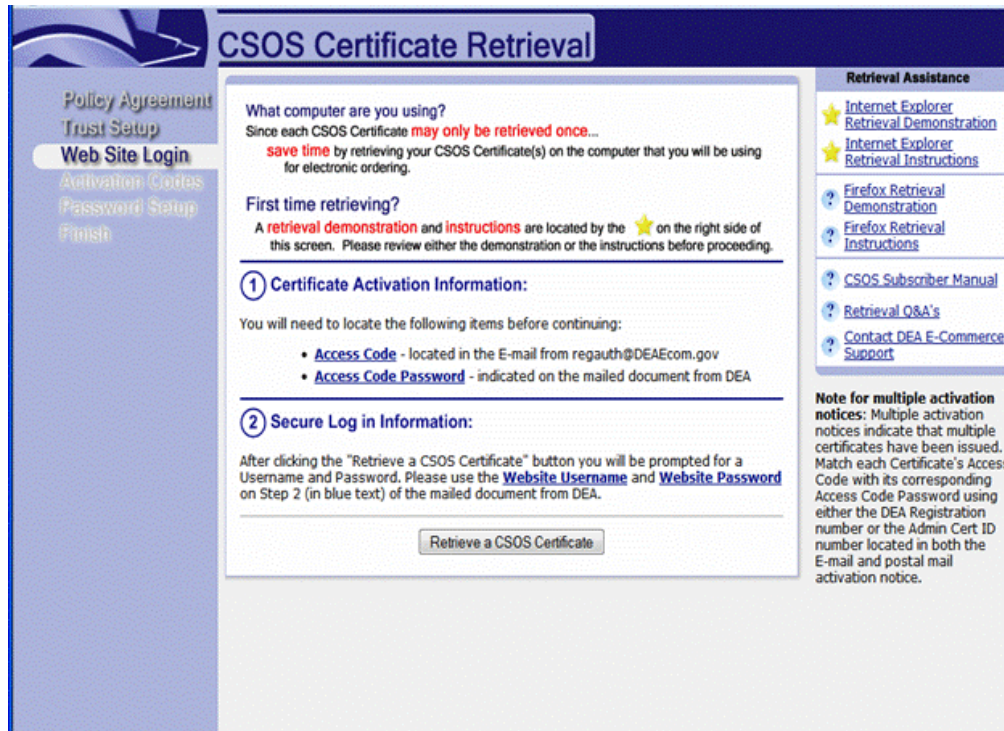


Figure 24: Website Login

3.1.3.1 Certificate Activation Information

In order to retrieve your CSOS certificate, the following items will be needed:

- Access Code - located in the Email from regauth@DEAecom.gov
- Access Code Password - indicated on the mailed document from DEA

Each certificate has a unique Access Code and Access Code Password. If you have received multiple postal mail activation notices, then there are multiple certificates to retrieve, each with a different Access Code and Access Code Password.

Match each Certificate's Access Code (the Email) with its corresponding Access Code Password (the postal mail document) using the DEA Registration number located in the Email.

3.1.3.2 Secure Log in Information

1. Click the **Retrieve a CSOS Certificate** button.

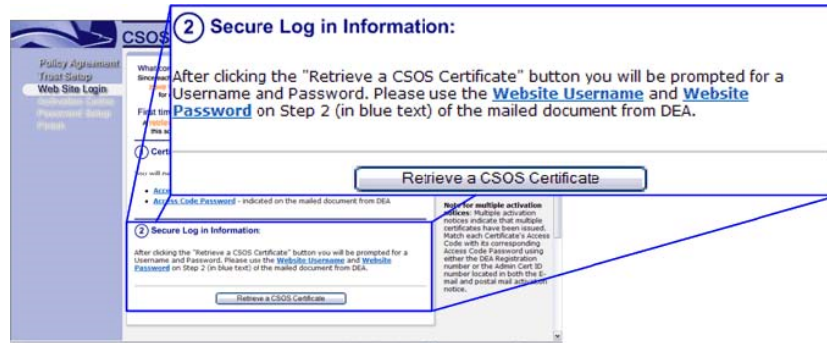


Figure 25: Secure Log in Information

2. Enter the Website Username and Website Password from Step 2 of the postal mail activation notice from DEA. The Password is cAsE sEnSiTiVe and may contain special characters such as @, #, and \$.

- Website Username: DEACERT3266
- Website Password: 4Cert2\$ign88



Figure 26: Certificate Warning

<p>IMPORTANT INFORMATION ON ACTIVATING YOUR CSOS CERTIFICATE Combine this information with the access code you received via E-Mail for this DEA Registration Number. Please retain this document for future management of your certificate.</p>	<p>DEA Diversion E-Commerce Support E-Mail: csosupport@DEAecom.gov Phone: 1-877-DEA-ECOM (1-877-332-3266)</p>										
<table style="width: 100%; border: none;"> <tr> <td style="width: 30%;">Name:</td> <td>John Smith</td> </tr> <tr> <td>E-Mail address:</td> <td>John.Smith@Internet.com</td> </tr> <tr> <td>CSOS Account Number:</td> <td>0000</td> </tr> <tr> <td>Certificate Serial Number:</td> <td>R00002005001</td> </tr> <tr> <td>CA Thumbprint (SHA-1):</td> <td>FERF F1 A8 F348 4ABD A146 E64R 5760 21C7 A A AR 43AF</td> </tr> </table>		Name:	John Smith	E-Mail address:	John.Smith@Internet.com	CSOS Account Number:	0000	Certificate Serial Number:	R00002005001	CA Thumbprint (SHA-1):	FERF F1 A8 F348 4ABD A146 E64R 5760 21C7 A A AR 43AF
Name:	John Smith										
E-Mail address:	John.Smith@Internet.com										
CSOS Account Number:	0000										
Certificate Serial Number:	R00002005001										
CA Thumbprint (SHA-1):	FERF F1 A8 F348 4ABD A146 E64R 5760 21C7 A A AR 43AF										
<p>Step 1 - Locate your E-Mail containing this same DEA Registration Number DEA Registration Number: XX1234567</p>											
<p>Step 2 - Use this information to log in to the DEA E-Commerce Certificate Retrieval Web page</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 30%;">Web site Address:</td> <td><Web site Address></td> </tr> <tr> <td>Web site Username:</td> <td><Web site Username></td> </tr> <tr> <td>Web site Password:</td> <td><Web site Password></td> </tr> </table>		Web site Address:	<Web site Address>	Web site Username:	<Web site Username>	Web site Password:	<Web site Password>				
Web site Address:	<Web site Address>										
Web site Username:	<Web site Username>										
Web site Password:	<Web site Password>										
<p>Step 3 - Use this Access Code Password, along with the Access Code from your E-Mail to activate your certificate</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 30%;">Access Code Password:</td> <td><Access Code Password></td> </tr> </table>		Access Code Password:	<Access Code Password>								
Access Code Password:	<Access Code Password>										

Figure 27: Website Username and Password

3.1.3.3 Enter Certificate Activation Information

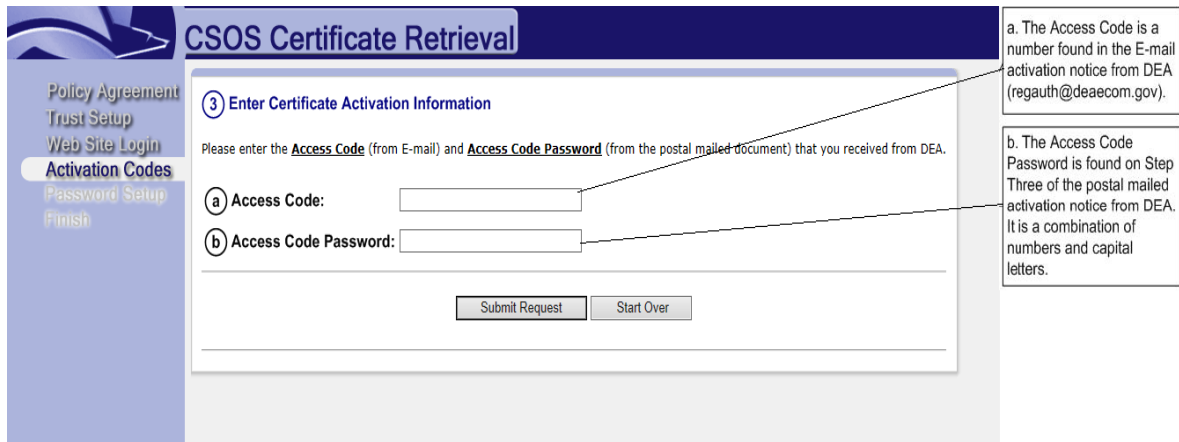


Figure 28: Enter Cert Activation Information

1. Enter the Access Code for this certificate. The Access Code may be found in the Email from DEA (regauth@deaecom.gov) and is specific to this certificate only.
2. Enter the Access Code Password for this certificate. The Access Code may be found in Step 3 of the postal mail document from DEA and is specific to this certificate only. The Access Code Password is a combination of numbers and letters separated by dashes (the dashes are optional).



IMPORTANT INFORMATION ON ACTIVATING YOUR CSOS CERTIFICATE
Combine this information with the access code you received via E-Mail from the DEA Registration Number. Please retain this document for future management of your certificate.

DEA Diversion E-Commerce Support
E-Mail: csosupport@DEAecom.gov
Phone: 1-877-DEA-ECOM (1-877-332-3366)

Name: John Smith
E-Mail address: John.Smith@Internet.com
CSOS Account Number: 8000
Certificate Serial Number: 300002005001
CA Thumbprint (SHA-1): FEBF F1A8 F348 4ABD A146 F64R 5760 21C7 AA AB43AF

Step 1 – Locate your E-Mail containing this same DEA Registration Number
DEA Registration Number: XX1234567

Step 2 – Use this information to log in to the DEA E-Commerce Certificate Retrieval Web page
Web site Address: <Web site Address>
Web site Username: <Web site Username>
Web site Password: <Web site Password>

Step 3 – Use this Access Code Password, along with the Access Code from your E-Mail to activate your certificate
Access Code Password: <Access Code Password>

Figure 29: Enter Access Code

3. Click the **Submit Request** button.

3.1.4 DEA E-Commerce CA Certificate

Note that installing a certificate into the computer's Certificate Store will depend on the requirements of the Distributor. This is only to be completed with direction from the Distributor.

3.1.4.1 Firefox

Firefox will store the CSOS user certificate as a password protected file located in the users Downloads directory (.p12 file). No additional security setup is required.

No other browser is supported by CSOS.

3.1.4.2 Enter a File Name and Password

1. Enter a descriptive filename in the **P12 File name** box.
2. Enter a new password and confirm the password.
3. Click the "Download the certificate as P12 file" link.

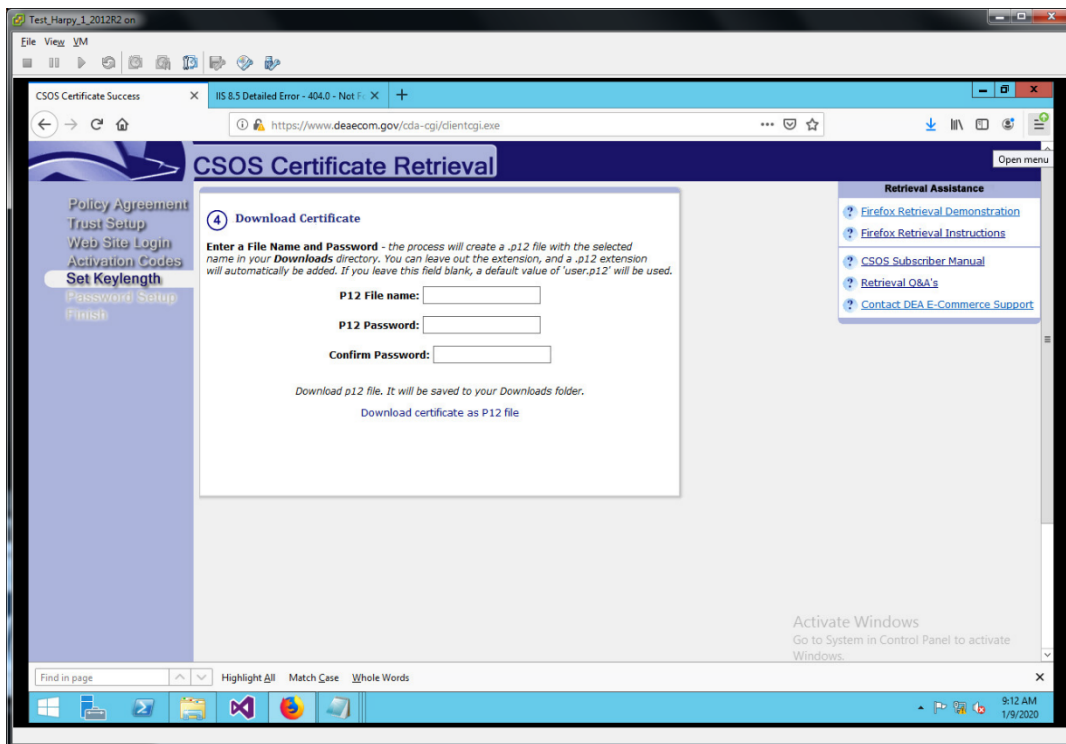


Figure 30: CSOS Certificate Retrieval

3.1.4.3 Save the Certificate to a .p12 File

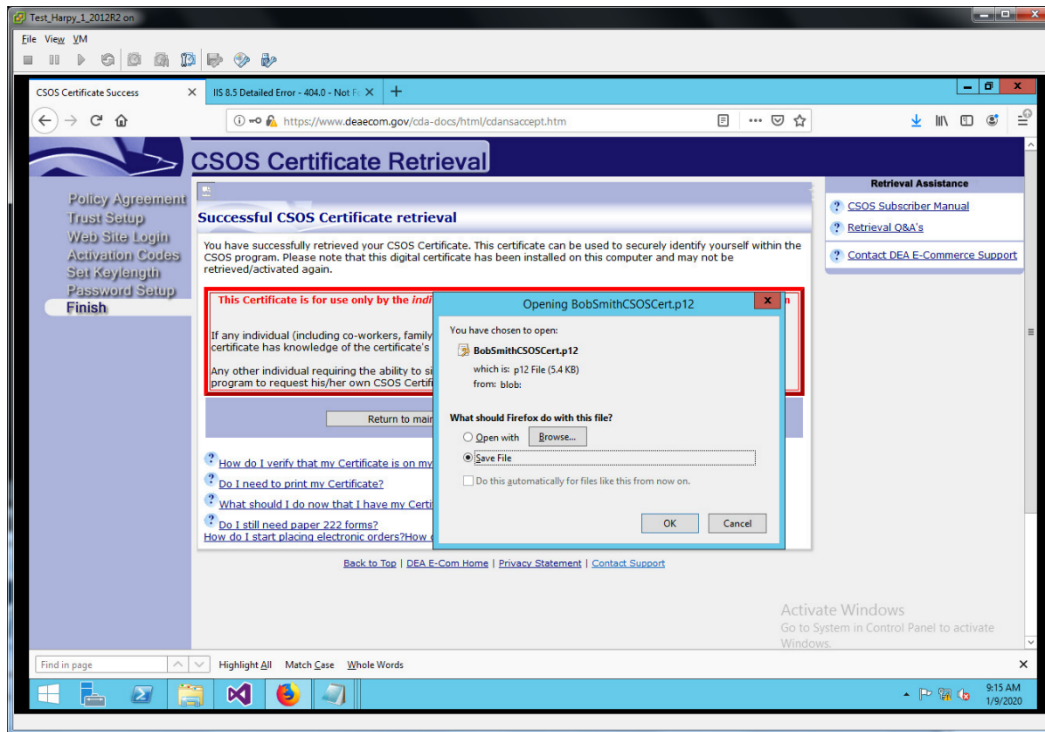


Figure 31: Save .p12 File

1. The Open Dialog will display.
2. Select **Save File**. Will be selected by default
3. Open Dialog Box will close and **Successful CSOS Certificate** will display.



Figure 32: Successful Retrieval

3.1.4.4 Load Certificate into the Certificate Store

Note that installing a certificate into the computer's Certificate Store will depend on the requirements of the Distributor. This is only to be completed with direction from the Distributor.

After Downloading the certificate to the Downloads Directory, the certificate may be loaded into the users certificate store. Some distributors require this; check with your distributor.

1. To start the loading of the certificate, double click the downloaded certificate xxxx.p12 file to start the Wizard.

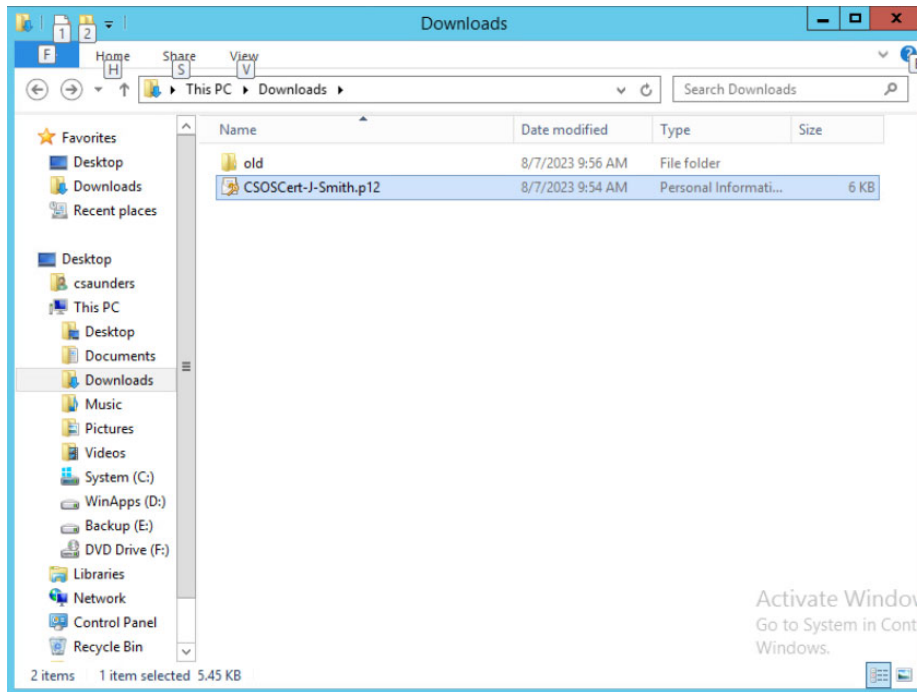


Figure 33: Downloaded Certificate

2. The "Certificate Import Wizard" will open. Select "Current User."

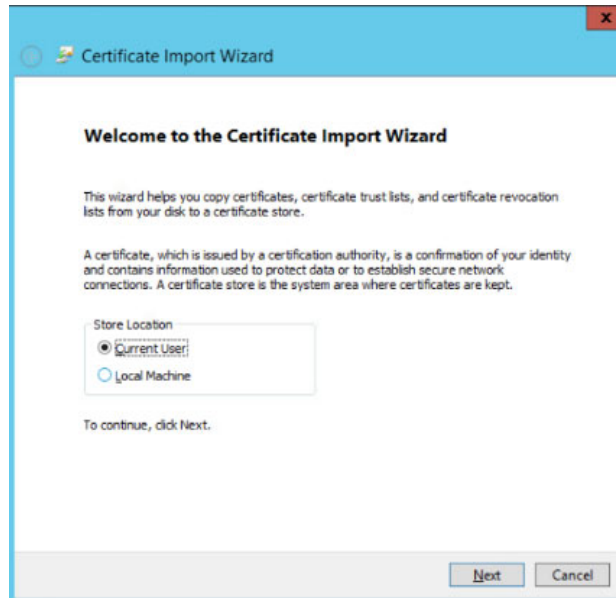


Figure 34: Certificate Import Wizard

- The .p12 file will be listed in the “File Name” field. Click “Next.”

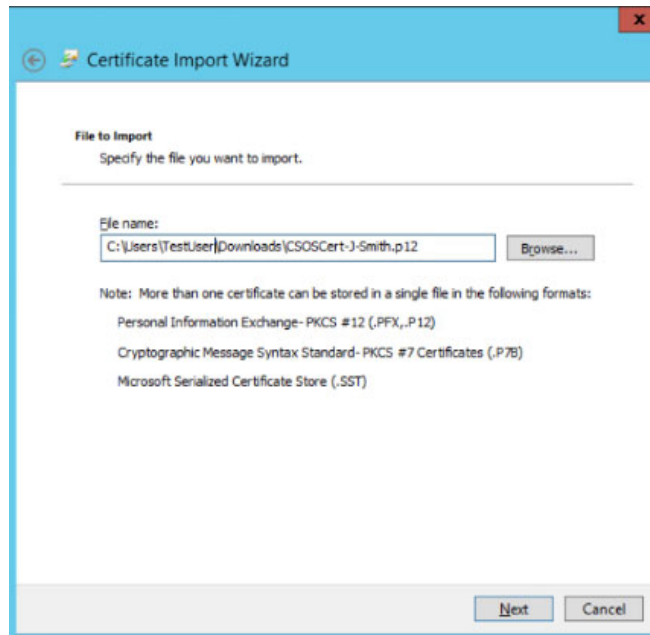


Figure 35: Specify File

- Enter the password of the .p12 file.
- Select “Mark this key as exportable....”
- Select “Include all extended properties”
- Click “Next.”

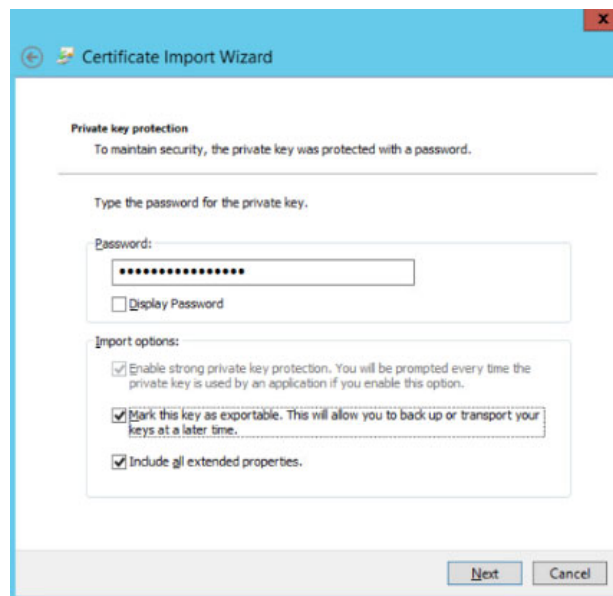


Figure 36: Import Options

- Select “Except the default “Automatic...”
- Click “Next.”

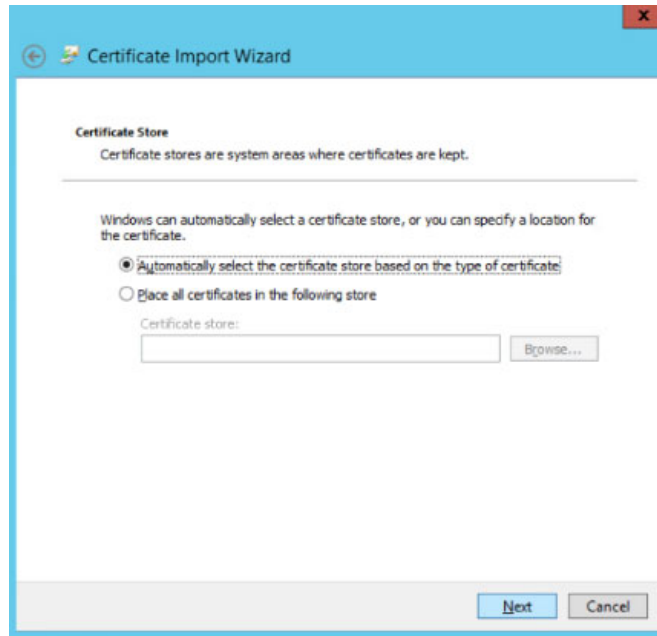


Figure 37: Select Certificate Store

10. Click “Finish”.

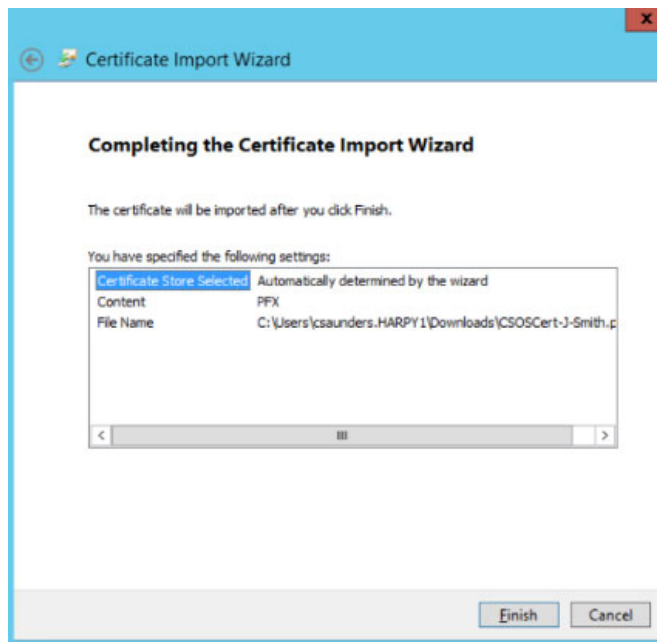


Figure 38: Finish Wizard

- At this point, a security level and password will need to be set. These will be required whenever the certificate is accessed. Select “Set Security Level.”



Figure 39: Import New Private Exchange Key

- Enter a new password. The computers password rules will apply. It can be the same as the .p12 file if it complies with the computers rules.
- Click “Finish.”

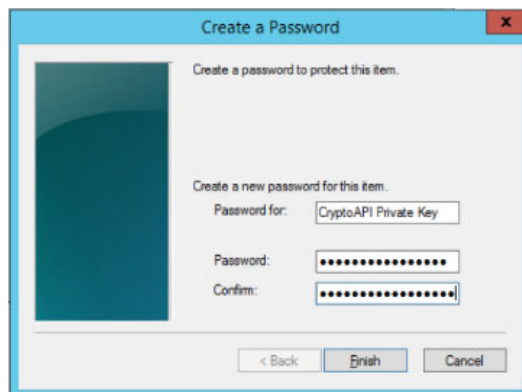


Figure 40: Create a Password

- Save the .p12 file to a storage device. The Certificate Import Wizard can be performed multiple times.

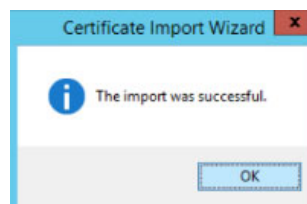


Figure 41: Import Successful

- To verify the certificate was imported, open “Microsoft Edge” browser.
- Select **Settings** from the Edge sprocket menu.
- Select **Privacy** from the options in the sidebar.
- Scroll down and select **Manage certificates**.

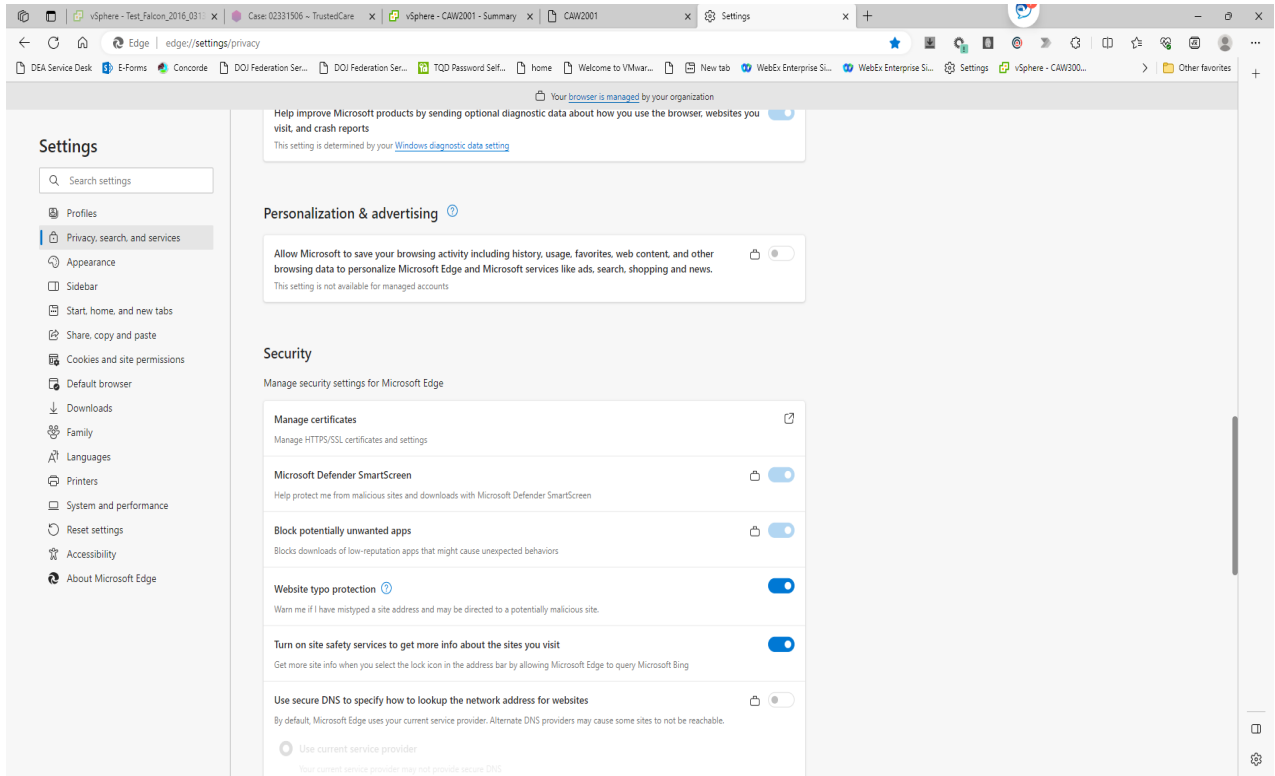


Figure 42: Edge Settings

19. Find the user’s name under “Issued too.”

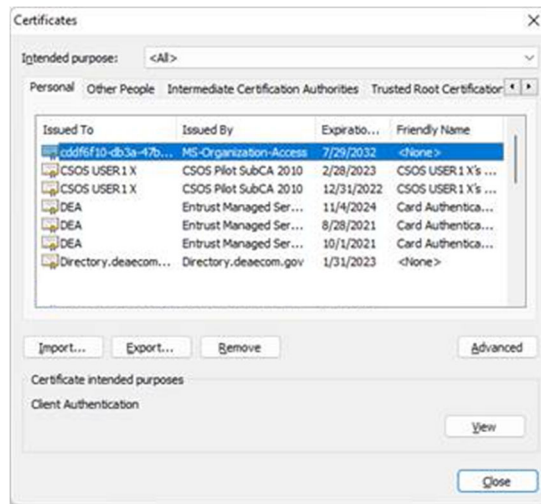


Figure 43: Installed Certificates

3.2 Certificate Denial

A certificate is no longer valid if the certificate has not been downloaded, installed, and activated after 60 days.

4.0 Other Website Actions

4.1 My Information Tab

4.1.1 Current DEA Registrations

A registrant must first create a primary Registrant account (approved by the CSOS RA Team) before any other accounts may be created.

All DEA number currently associated with your account will be displayed in the **Current DEA Registrations** tab. Note that the Current DEA Registrations tab will display an Empty message if:

- Either no active certificate data was pulled from the legacy CSOS database
- No request was made
- No request was approved

DEA Registration Number	Serial Number	Role	Status	Provision Date	Expiration Date	Business Name	Business Address	Organization Address
		Power of Attorney (POA)	ACTIVE					

Figure 44: Current DEA Registrations

- **DEA Registration Number:** the DEA registration number assigned to the listed role
- **Serial Number:** the unique identifier for the CSOS certificate
- **Role:** the role of the listed subscriber
- **Provision Date:** the date on which the certificate request was approved
- **Expiration Date:** the date on which the certificate will expire
- **Business Name:** the name of the business associated with the subscriber
- **Business Address:** the name of the address from which the named business operates
- **Organization Address:** if different from the business address, the address from which the parent chain company operates

4.1.2 Renew

Perform the following the steps to renew a certificate

The screenshot shows a web interface for creating a request. At the top, there are three tabs: 'Current DEA Registrations', 'Status of Requests', and 'Create Request'. The 'Create Request' tab is active. Below the tabs, there is a form with the following fields:

- Request Type ***: A dropdown menu with 'Renew' selected. An information icon (i) is to the right.
- Comments**: A text input field.
- DEA Registration Number List**: A section containing a table with one row. The first column is 'DEA Registration # *' with a blurred value and a checkbox. The second column is 'Expiration Date' with the value 'May 20, 2023'. The third column is 'Role' with the value 'Registrant'.

At the bottom left of the form, it says 'Status: NEW'.

Figure 45: Renew

1. Select **Renew** from the *Request Type* menu.
2. Add any addition comments relevant to the created request in the *Comments* field.
3. Select all DEA numbers to be renewed.
 - a. Note that more than one DEA number may selected, allowing multiple numbers to be renewed in bulk.
4. Click the **Validate and Save** button to validate the added DEA number(s).
 - a. If the DEA Number does not pass validation, this will be reported. Consult the Validation Troubleshooting table (section 4.1.4) to resolve the issue.
5. Click the **Submit** button.

4.1.3 Revoke

Perform the following steps to revoke a certificate:

The screenshot shows a web form for creating a registrant enrollment request. The 'Request Type' dropdown is set to 'Revoke' and the 'Justification' dropdown is set to 'Other'. There is a text input field for 'Comments'. Below this is a section titled 'DEA Registration Number List' with a 'Select All' checkbox. Underneath is a table with one row containing a 'DEA Registration # *' and a 'Role' of 'Registrant'. The 'Status' is 'NEW'. At the bottom are two buttons: 'VALIDATE AND SAVE' and 'SUBMIT'. A note at the bottom left states '* fields are required.'

Figure 46: Create Registrant Enrollment Request

1. Select **Revoke** from the *Request Type* menu.
2. Select a justification for the revocation from the *Justification* menu.
 - a. **Affiliation Change:** the subscriber is no longer with the organization
 - b. **CA Compromise:** your registered Certificate Authority has become compromised
 - c. **Cessation of Operation:** your organization has gone out of business
 - d. **Key Compromise:** your certificate key has been compromised
 - e. **Superseded:** the user has been replaced by another user
 - f. **Other:** any other reason. Note you will be required to provide the reason in a **Comment** field if *Other* is selected
3. Add any addition comments relevant to the created request in the *Comments* field.
4. Select all DEA numbers to be revoked.
5. Click the **Validate and Save** button to validate the added DEA number(s).
 - a. If the DEA Number does not pass validation, this will be reported. Consult the Validation Troubleshooting table (section 4.1.4) to resolve the issue.
6. Click the **Submit** button.

4.1.4 Validation Troubleshooting

The following table shows the possible errors you might receive when validating a DEA Number, and the correct methods to resolve them.

Error	How to Resolve
DEA number has expired	Choose an active, unexpired DEA number. OR Renew the expired DEA number through the DEA Registration application (https://apps.deadiversion.usdoj.gov/webforms2/spring/renewalLogin)
DEA number has retired	Choose an active, unretired DEA number.
This role is already taken.	Only one principal coordinator and one alternate coordinator. Please select either the registrant or POA role.
Please enroll register REGISTRANT user first.	Enroll as the primary registrant. Note that this may only be approved by a government RA.
Contact your primary Registrant to create their profiles.	The First Registrant role is missing. Ask your primary registrant to create his or her profile.
Cannot apply for this role because REGISTRANT/PRINCIPLE COORDINATOR is taken	Select another role other than the one previously selected
Cannot apply for this role because REGISTRANT/ALTERNATE COORDINATOR is taken	Select another role other than the one previously selected
Cannot apply for this role because PRINCIPAL COORDINATOR is taken	Select another role other than the one previously selected
Cannot apply for this role because ALTERNATE COORDINATOR is taken	Select another role other than the one previously selected
User already has a role for this DEA number	Select another role other than the one previously selected
We require one of the following roles to be created or migrated to our system first.	Select one of the following: <ul style="list-style-type: none"> • PRINCIPAL COORDINATOR, NO SIGNING CERTIFICATE • REGISTRANT/ PRINCIPAL COORDINATOR • PRINCIPAL COORDINATOR WITH SIGNING CERTIFICATE

Error	How to Resolve
PRINCIPAL COORDINATOR, NO SIGNING CERTIFICATE, REGISTRANT/PRINCIPLE COORDINATOR, PRINCIPAL COORDINATOR WITH SIGNING CERTIFICATE, ALTERNATE COORDINATOR, NO SIGNING CERTIFICATE, ALTERNATE COORDINATOR WITH SIGNING CERTIFICATE, or REGISTRANT	<ul style="list-style-type: none"> • ALTERNATE COORDINATOR, NO SIGNING CERTIFICATE • ALTERNATE COORDINATOR WITH SIGNING CERTIFICATE • REGISTRANT
A request for this role is in review	Select another role OR Contact your PRIMARY REGISTRANT to approve your request OR Wait for the government RA to approve your request
User has sent request for this DEA number. The request is in review.	Select another role OR Contact your PRIMARY REGISTRANT to approve your request OR Wait for the government RA to approve your request

4.2 Registrants and Coordinators Tab

Once requests are made by the subscriber, the RA or RA-approved registrant will receive an email to confirm that a request was created. You will have to review, approve, or reject the request.

You may only see the DEA numbers in this tab to which you are registered as an active Registrant or Principal Coordinator.

Click the **Review/Approve/Reject** link. CSOS will open the **Request Approval Form** (see next page).

4.2.1 Member Approvals

Action	Review/Approve/Reject Link	Request Id	Request Type	Role	Beneficiary Information	Updated Date	Requestor Email
COLLAPSE ▾	Review/Approve/Reject		ENROLL	Principal Coordinator - without Signing Cert		Apr 26, 2023	

DEA Registration Numbers: [REDACTED]

Figure 47: Member Approvals Tab

- **Action:** you may select **Collapse** or **Expand** the record's menu to collapse or expand the record
- **Review/Approve/Reject Link:** click this link to open the Approve/Reject Approval Form (see next page)
- **Request ID:** the unique ID number assigned to the request
- **Request Type:** the type of request pending approval currently listed
- **Role:** the role of the listed subscriber
- **Subscriber Information:** the subscriber who made the request
- **Updated Date:** the date on which the request was last updated
- **Requestor Email:** the email of the individual who made the request

1. Enter any comments pertinent to the request,
 - a. If you wish to approve the request, click the **Approve Request** button.
 - b. If you wish to reject the request, click the **Reject Request** button.
2. Once you click the **Approve** or **Reject** buttons, the record will be removed from the *Member Approvals* tab.

Request Approval Form

The following user has requested a certificate for the below DEA registration(s).

Request Date:
04-26-2023

Requester First Name:
JOHN

Requester Last Name:
SMITH

Requester Email:

Requested Certificate:
Registrant

Registration Number(s):

Requester Comments:

Approver Comments:

Comments:
Approved

Figure 48: Request Approval Form

4.2.2 Member Revocations

This tool is used to revoke a subscriber's certificate. To perform this task, you must either be a CSOS-approved Registrant or a Coordinator.

The screenshot shows the 'Member Revocations' tab selected. At the top, there are three tabs: 'Member Approvals', 'Member Revocations', and 'Status of Requests'. Below the tabs, there are two dropdown menus: 'Request Type *:' set to 'Revoke' and 'Justification *:' set to 'Affiliation Change'. Below these is a 'Search User Certificates' section with five input fields: 'First Name:', 'Last Name:', 'Email:', 'Serial Number:', and 'DEA Registration Number:'. Below the search fields is a 'Revoke List' table with columns for 'DEA Registration Number', 'Role', 'First Name', 'Last Name', and 'Email'. The table contains one row with a checkbox, a blurred DEA number, and the role 'Principal Coordinator - without Signing Cert'. At the bottom left of the form is a 'SUBMIT' button. A note at the bottom left states '* fields are required.'

Figure 49: Member Revocations Tab

1. Select the justification for the revocation from the following:
 - a. **Affiliation Change:** the subscriber is no longer with the organization
 - b. **CA Compromise:** your registered Certificate Authority has become compromised
 - c. **Cessation of Operation:** your organization has gone out of business
 - d. **Key Compromise:** your certificate key has been compromised
 - e. **Superseded:** the user has been replaced by another user
 - f. **Other:** any other reason. Note you will be required to provide the reason in a **Comment** field if *Other* is selected
2. Search for a user's certificate. The more fields that are filled, the fewer results will be returned. At least one field must be filled with valid data to return a result.
 - **First Name:** the subscriber's first name
 - **Last Name:** the subscriber's last name
 - **Email:** the subscriber's email address
 - **DEA Registration Number:** the subscriber's DEA number
 - **Serial Number:** the serial number associated with the subscriber's record

As a general rule:

 - *if you want a location, enter a DEA Number,*
 - *if you want a certificate, enter a first name, last name, or serial number.*
3. Check the checkboxes for any records you wish to be revoked.
4. Click the **Submit** button.

4.2.3 Status of Requests

The status of any request made is available in the **Status of Requests**

Action	Request Id	Request Type	Role	Status	Comments	Beneficiary Information	Updated Date	Requestor Email
COLLAPSE ▾		ENROLL	Principal Coordinator - without Signing Cert	CERTIFICATE GENERATION IN PROCESS	Approved		Apr 26, 2023	
DEA Registration Numbers: [REDACTED]								

Figure 50: Status of Requests

- **Action:** you may select **Collapse** or **Expand** from the record's menu to collapse or expand the record
- **Request ID:** the unique ID number assigned to the request
- **Request Type:** the type of request pending approval currently listed
- **Role:** the role of the listed subscriber
- **Status:** the current status of the request
- **Comments:** comments made by the approving authority
- **Beneficiary Information:** the name of the listed beneficiary
- **Updated Date:** the date on which the request was last updated
- **Requestor Email:** the email of the individual who made the request

4.2.4 Password Reset

Note: this section is provided so that Helpdesk personnel may guide subscribers in resetting their passwords, if necessary.

To reset your password:

1. At the *Login screen* click the **Sign in** button.

Login

Instructions: Select a login method to continue

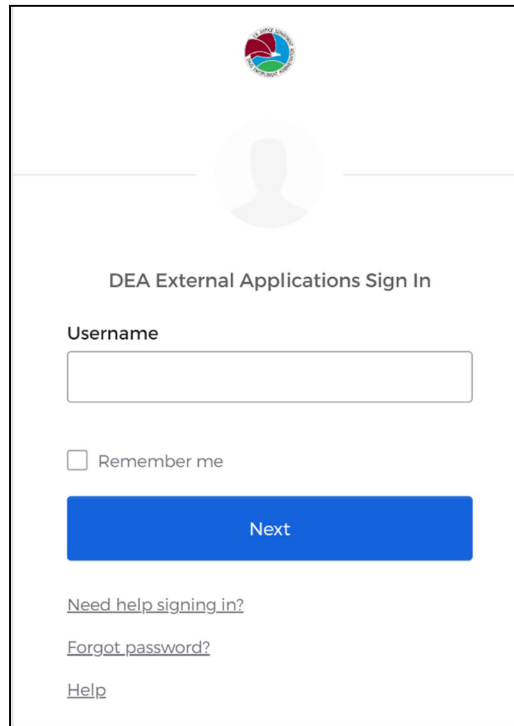
SIGN IN

SIGN UP

Having trouble logging in? Contact CSOS Service Desk at (800) 111-8729 or CSOS.TECHNOLOGY.SERVICE.DESK@doj.gov for assistance.

Figure 51: Login

2. Click the *Forgot password?* Link.



DEA External Applications Sign In

Username

Remember me

Next

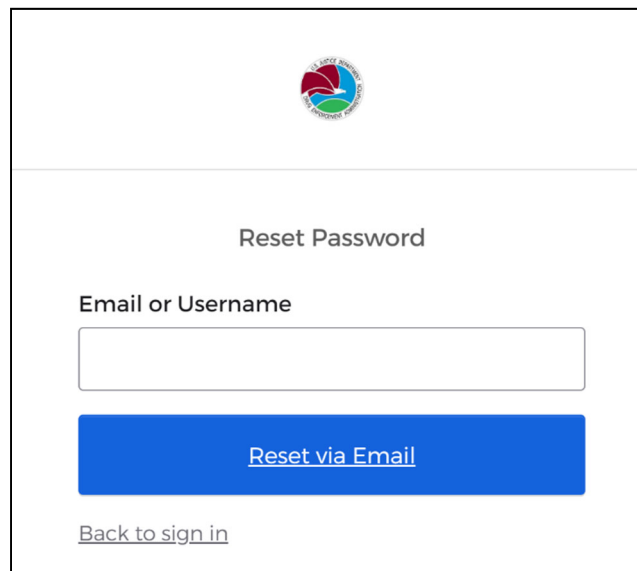
[Need help signing in?](#)

[Forgot password?](#)

[Help](#)

Figure 52: Username

3. Enter your email address or username, and click the **Reset via Email** button.



Reset Password

Email or Username

Reset via Email

[Back to sign in](#)

Figure 53: Reset Password

You will receive emails from Okta informing you that your password request has been sent. It will include a link to following to continue the process.

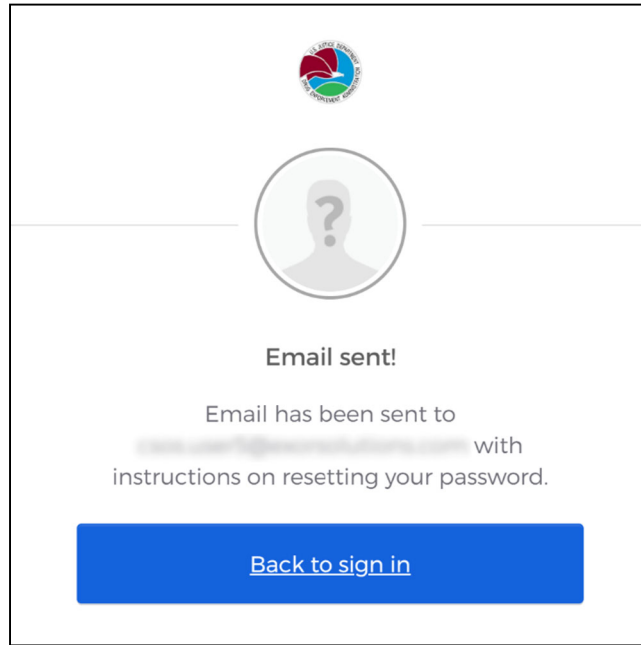


Figure 54: Email Sent

4. Click the link in the email to continue.

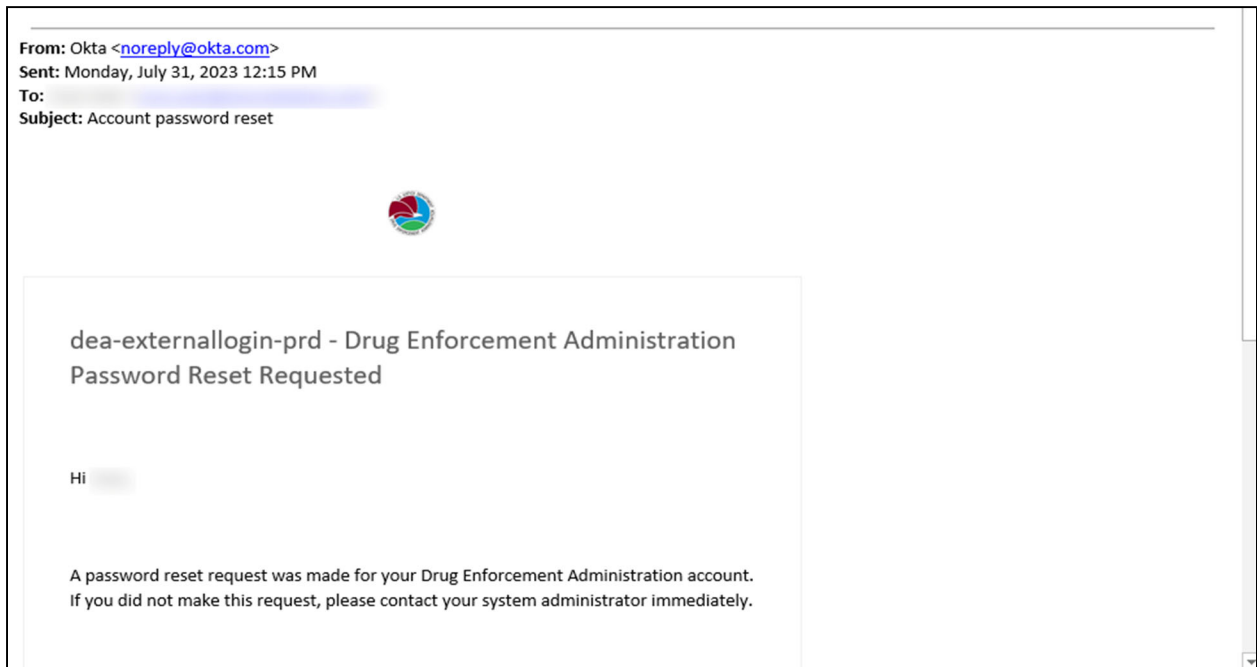
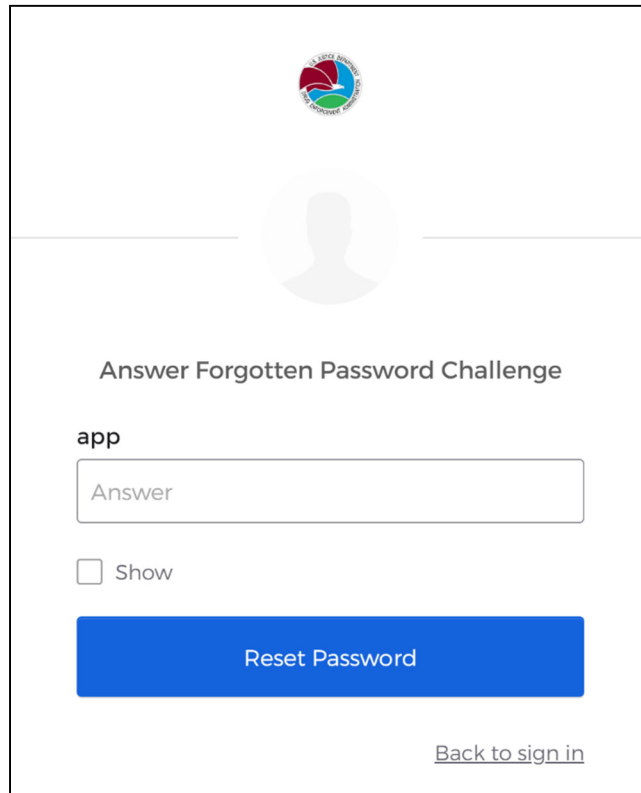


Figure 55: Reset Requested

5. Answer the challenge question that you previously established to verify your identity.



The screenshot shows a web form for a password challenge. At the top center is a circular logo with a stylized 'S' and 'C' and the text 'SOUTH COAST COMMUNITY COLLEGE'. Below the logo is a grey silhouette of a person's head and shoulders. The main heading is 'Answer Forgotten Password Challenge'. Underneath, the word 'app' is displayed. There is a text input field containing the word 'Answer'. Below the input field is a checkbox labeled 'Show'. A large blue button with the text 'Reset Password' is positioned below the checkbox. In the bottom right corner, there is a link that says 'Back to sign in'.

Figure 56: Challenge Question

6. Enter your new password in the fields provided. Optionally, you may check the box to sign yourself out of all other devices.

Reset your Okta password

Password requirements:

- At least 10 characters
- A lowercase letter
- An uppercase letter
- A number
- No parts of your username
- Your password cannot be any of your last 10 passwords

New password

Repeat password

Sign me out of all other devices.

Reset Password

Figure 57: Reset Password

You will receive emails from Okta informing you that your password request has been received, and a second one once the password has been changed.

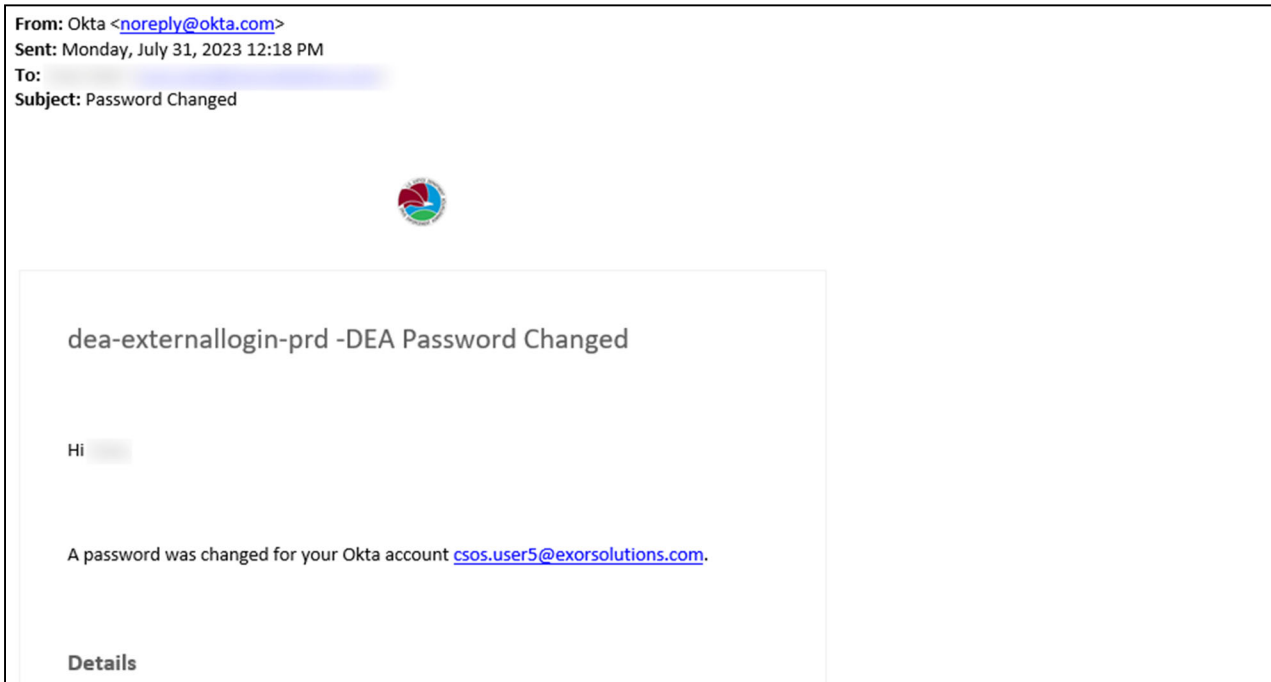


Figure 58: Password Reset

5.0 Certificate Management

5.1 Certificate Renewal

Certificate Renewal is the process of DEA issuing a **new** certificate to a subscriber. The subscriber will be issued new activation codes and must retrieve the new certificate via DEA's secure certificate retrieval Web site.

All CSOS digital certificates have an expiration date after which the certificate will no longer be valid for electronic ordering or digitally signing communications.

- **CSOS Signing Certificates** expire when the associated DEA Registration expires.

Signing Certificates must be renewed in addition to the DEA Registration.

CSOS sends an E-mail notifying the Subscriber and the Subscriber's CSOS Coordinator 45 days prior to the expiration date of the Subscriber's CSOS certificate. The Subscriber or Registrant/Coordinator is responsible for renewing the certificate and is provided Certificate renewal instructions with the E-mail notice. Failure to renew a CSOS Signing Certificate will result in an inability to sign electronic orders for controlled substances.

There are two types of renewal methods for CSOS Certificates.

- **Electronic renewal may be used twice** – After initial enrollment to login.gov, subscribers may complete renewal electronically no more than two (2) times.
- **Initial enrollment must be used the third time** - Subscribers are required to reestablish identity using the initial registration process (login.gov).

5.2 Certificate Revocation

Certificate revocation results in the loss of ability of the digital certificate holder to use the certificate for electronic ordering purposes by placing the certificate information onto a “Certificate Revocation List,” or CRL. Suppliers are required to check each digitally signed order to ensure that the certificate associated with the digital signature has not expired or been revoked. Revoked certificates appear on a CRL within 24 hours of acknowledgement by DEA Diversion E-Commerce Support, or within six (6) hours of if the revocation reason is due to known or suspected compromise of the private key.

5.2.1 Revocation Reasons

A Subscriber’s certificate may/will be revoked under the following circumstances:

- The subscriber (certificate holder) no longer orders controlled substances and/or is no longer employed by the organization associated with the Certificate’s DEA Registration number
- Subscriber information contained in the certificate has changed including legal name changes and E-mail address changes
- DEA Registration (as indicated on the paper DEA Registration Certificate, Form DEA-223) information has changed including DEA Registration name, number, address, or authorized ordering schedules are reduced
- DEA posts notice that certificate holder’s DEA Registration has been revoked, suspended or restricted, that the Registration information has changed, or that the Registration has been terminated
- It can be demonstrated that the Subscriber has violated the stipulations of the Subscriber Agreement
- The private key is lost, compromise is suspected, or cannot be accessed for any reason (the private key used when digitally signing a document is activated by a password or token under the Subscriber’s sole control, so it is important not to divulge this information to anyone, even your Registrant or CSOS Coordinator)
- The Subscriber, the DEA Registrant under whose Registration a certificate holder obtained a certificate, or CSOS Coordinator requests that the affiliated Subscriber certificate be revoked

Official policy regarding Certificate revocations may be found in the E-Commerce Certificate Policy available on <https://www.deacom.gov/>.

5.2.2 Procedure for Revocation Requests

The DEA E-Commerce Web site (<https://www.deaecom.gov>) contains the portal used to revoke active certificates (see 4.1.3 and 4.2.2). Registrants and Coordinators have the ability complete certificate revocations.

Assistance is available from the CSOS Helpdesk by telephone: 1-877-DEA-ECOM (1-877-332-3266).

In the event of suspected compromise, revoke the suspected certificate, and call the CSOS Helpdesk to report the issue.

5.3 Certificate Information

5.3.1 View/Open the certificate

A CSOS Certificate must be opened in order to view the data it contains about its owner and associated information. View the DEA extension in the certificate

Each extension or Field in the certificate is shown in the left column of the Certificate's details tab. The Certificate's associated value for that field is displayed in the Value column as well as the bottom pane when a field is selected. The below table should be used to interpret the Field ("object identifier") number to a readable DEA extension name. This section of the Subscriber Manual documents how to interpret and verify the data contained in a CSOS Certificate.

Table 1: Certificate Field Value Mapping to DEA Extension Name

Certificate Field Value (object identifier)	DEA Extension Name
2.16.840.1.101.3.5.1	DEA Certificate Version Number
2.16.840.1.101.3.5.2	DEA Registrant Name
2.16.840.1.101.3.5.4	DEA Schedules
2.16.840.1.101.3.5.5	DEA Business Activity
2.16.840.1.101.3.5.6	DEA Registered Postal Address
2.16.840.1.101.3.5.7	Hashed DEA Registration Number (SHA-2)

5.3.2 DEA Certificate Version Number Information

The DEA Certificate Version Number Information extension allows relying party applications to identify the DEA profile version being used by the particular certificate. This enables multiple profile versions to be used at the same time without ambiguity.

The value of the extension is displayed as a hexadecimal value. The DEA Certificate Version Number Information value is the last two characters (i.e. 00) of the extension value. The current value is fixed at 0 to represent version 1 of the DEA certificate profile.

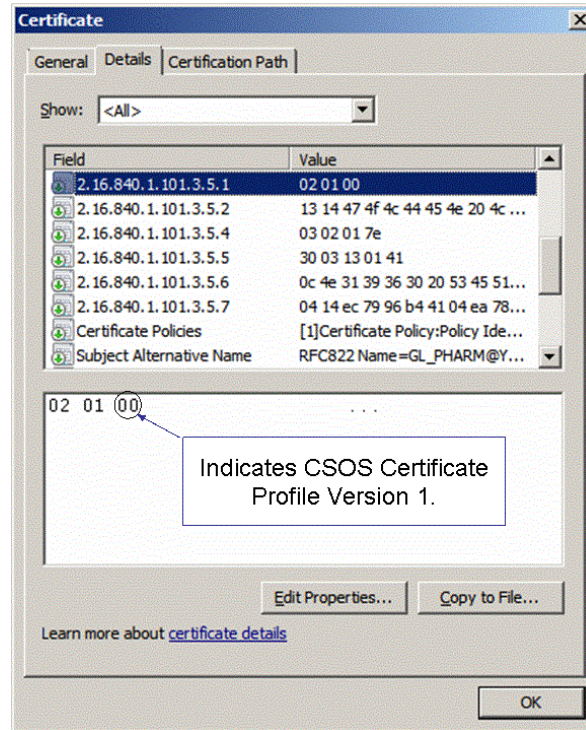


Figure 59: DEA Certificate Profile Version

In the above figure, the DEA certificate profile version extension value is 00, which is Version 1.

5.3.3 DEA Registrant Name

The DEA Registrant Name extension is used to identify the DEA Registrant for which a CSOS Signing Certificate is associated. Example: *last name, first name middle initial (Doe, John A)* or *business name (Acme, Inc.)*.

Highlight section 2.16.840.1.101.3.5.2 to view the associated Registrant Name, as displayed below in Figure 3.

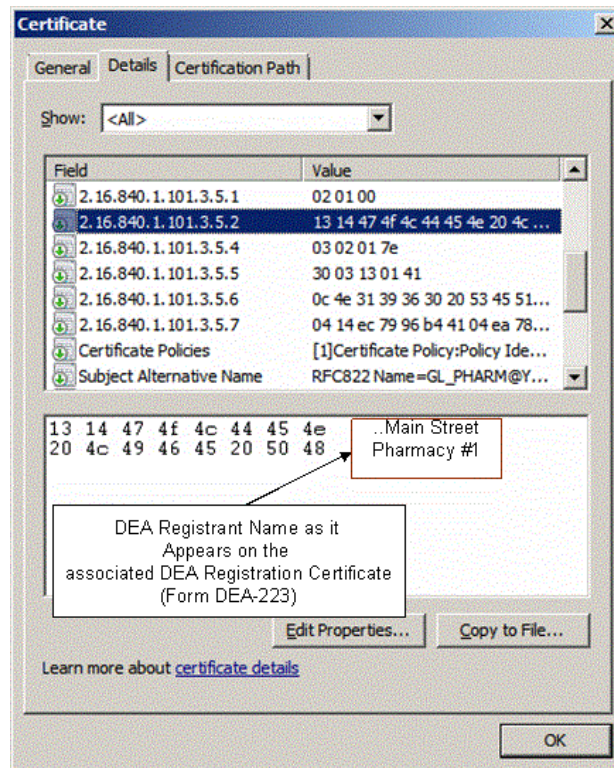


Figure 60: DEA Registration Name

5.3.4 DEA Schedules

The *DEA Schedules* extension reflects the controlled substance schedules the certificate owner is authorized to prescribe or dispense.

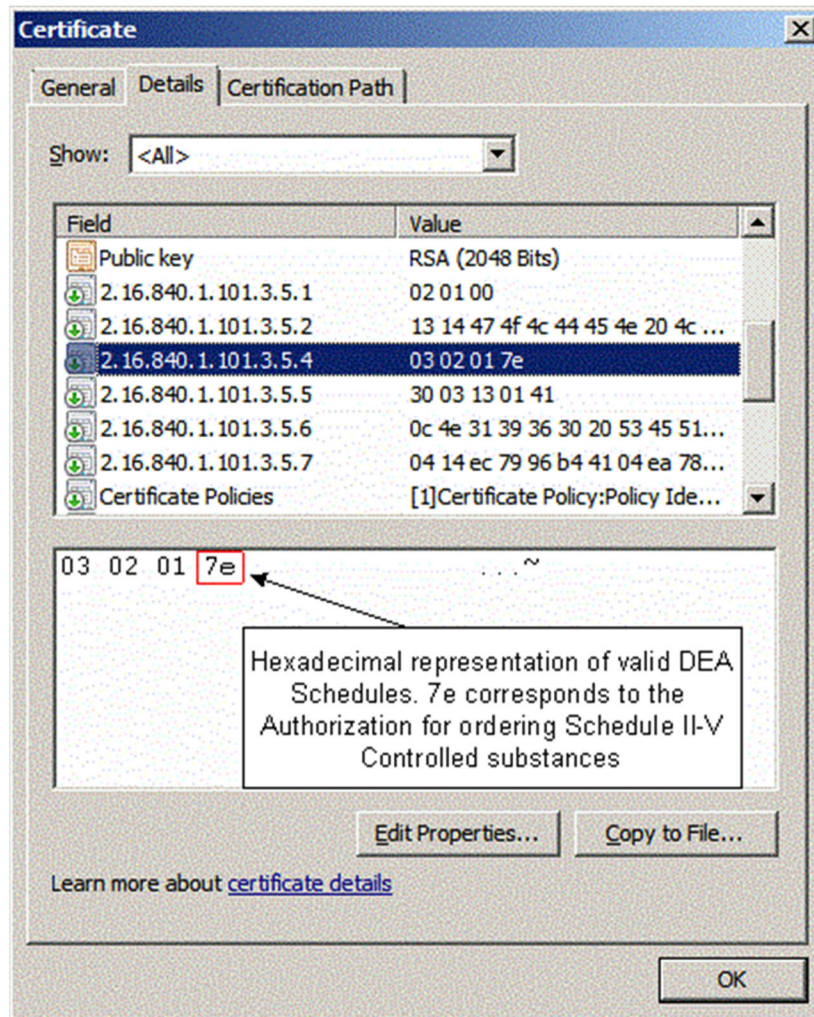


Figure 61: DEA Schedule Extension

In the above figure, the DEA schedule extension value is 7E. '7E' represents a hexadecimal number (Base-16 rather than the standard base-10 counting system). When translated to binary (Base-2), the allowable ordering schedules can be determined. **Since the majority of CSOS Signing Certificates are issued for schedules II-V (2, 2N, 3, 3N, 4, and 5), this translation will not be necessary if your Certificate's associated DEA Registration number is authorized for these schedules.**

5.3.5 Convert a Hexadecimal to Binary

Use the last two characters of the Certificate Extension Value as shown in Figure 4. Using each of the two characters separately, the following conversion table allows the associated binary value to be determined.

Table 2: Hex to binary conversion table

Hex Value	Binary Value			
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
A	1	0	1	0
B	1	0	1	1
C	1	1	0	0
D	1	1	0	1
E	1	1	1	0
F	1	1	1	1

Using the above conversion table for an extension value of '7E':

- Hexadecimal value of **7** translates to the binary **0111**.
- Hexadecimal value **E** translates to binary **1110**.
- Combining the two binary values results in **01111110**.

The resulting binary number (i.e. 01111110) can be used to determine the authorized ordering Schedules. Each 0 or 1, called a 'bit', represents a DEA Schedule. Reading from left to right, each bit has a position (position 0 through 7), which maps to a DEA Schedule as documented in Figure 6.

- A 0 bit indicates an unauthorized schedule.
- A 1 bit indicates an authorized schedule.

The table below provides a mapping of allowable schedules to bits in the DEA schedule extension.

Table 3: Controlled Substance Schedule Bit

Bit	Schedule	
0	Schedule I Narcotic and Non-narcotic	1
1	Schedule II Narcotic	2
2	Schedule II Non-narcotic	2n
3	Schedule III Narcotic	3
4	Schedule III Non-narcotic	3n
5	Schedule IV	4
6	Schedule V	5
7	Unused	N/A

The table below displays sample schedule to bit to hex value mappings.

Table 4: DEA extension value conversion table

Bit field	0	1	2	3	4	5	6	7	Decimal	HEX
Schedules	1	2	2n	3	3n	4	5	Unused		
2,2n,3,3n,4,5	0	1	1	1	1	1	1	0	126	7 E
2, 3,3n,4,5	0	1	0	1	1	1	1	0	94	5 E
2n,3,3n,4,5	0	0	1	1	1	1	1	0	62	3 E
2	0	1	0	0	0	0	0	0	64	4 0
2n	0	0	1	0	0	0	0	0	32	2 0
3n 4 5	0	0	0	0	1	1	1	0	14	0 E
2n 3n 4 5	0	0	1	0	1	1	1	0	46	2 E

5.3.6 DEA Business Activity

The *DEA Business Activity* extension identifies the business classification of the CSOS Subscriber's associated DEA Registration. The DEA Business Activity code must be consistent with the associated DEA Registration Certificate (Form DEA-223).

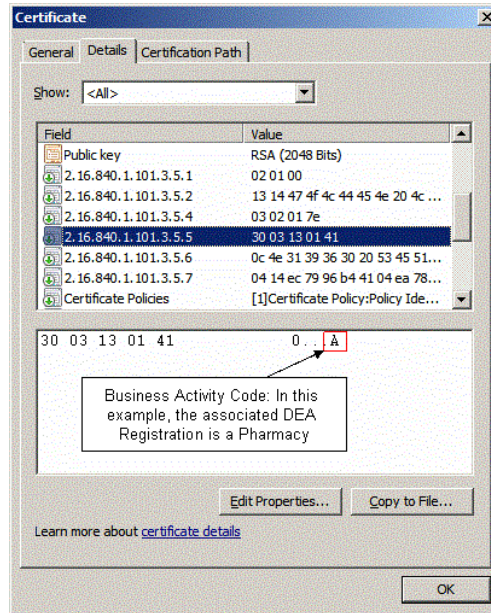


Figure 62: DEA Business Activity Code

Table 5: DEA Business Activity Codes for CSOS

Business Activity	Code
Pharmacy	A
Hospital/Clinic	B
Practitioner	C
Teaching Institution	D
Manufacturer	E
Distributor	F
Researcher	G
Analytical Lab	H
Exporter	K
Mid-Level Practitioner	M
Narcotic Treatment Programs	
Maintenance	N

Business Activity	Code
Detoxification	P
Maintenance & Detoxification	R
Compounder/Maintenance	S
Compounder/Detoxification	T
Compounder/Maint. & Detox	U

5.3.7 DEA Postal Address

The *DEA postal address* Certificate extension identifies associated DEA Registration’s postal address as it is registered with DEA.

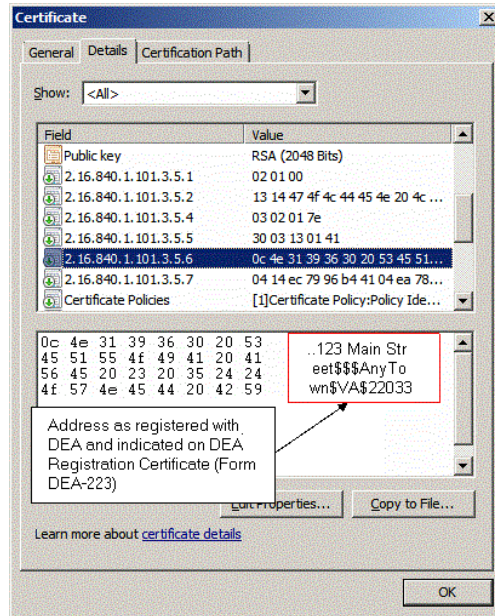


Figure 63: DEA Registered Postal Address Extension

The resulting extension value takes the format of: Address 1\$Address 2\$Address 3\$City\$State\$Zip Code as documented in the table below.

Table 6: DEA Postal Address Example Values

CSA Database Field	CSA Database value
Example 1	
Address 1	Dept 1
Address 2	123 Main Street
Address 3	PO Box 45678
City	Home Town
State	MD
Zip Code	12345-6789
Extension Value	Dept 1\$123 Main Street\$PO Box 45678\$Home Town\$MD\$12345-6789
Example 2	
Address 1	123 Main Street

CSA Database Field	CSA Database value
Address 2	
Address 3	
City	Home Town
State	MD
Zip Code	12345-6789
Extension Value	123 Main Street \$\$\$Home Town\$MD\$12345-6789

5.3.8 DEA Registration Number

For privacy reasons, a CSOS Signing Certificate’s associated DEA Registration number does not appear in clear text in the Certificate. The DEA Registration number, along with the Certificate Serial Number, are hashed together and included in the Certificate Field 2.16.840.1.101.3.5.7. Using a hash (an irreversible encoding), the DEA Registration number may be verified only if it is already known. Since the purchaser’s DEA Registration number is included in all CSOS transactions, the supplier may use the given Registration Number from the order along with the Certificate’s Serial Number to determine the validity of the DEA Registration Number in the Certificate used to digitally sign the order.

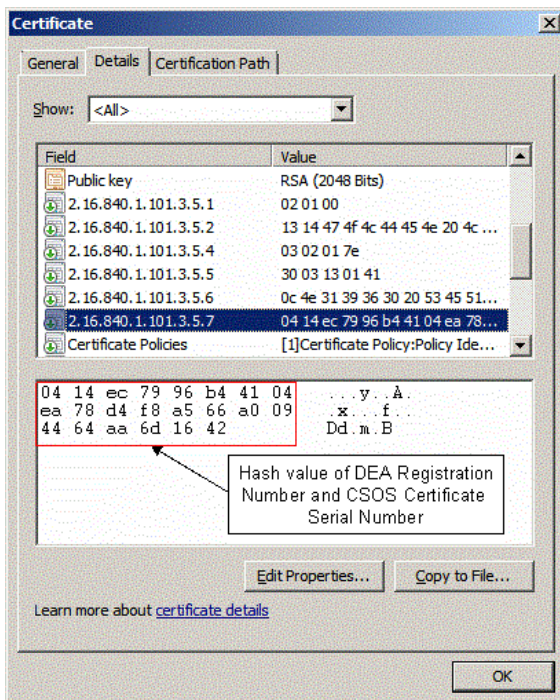


Figure 64: Hashed DEA Registration Number Extension

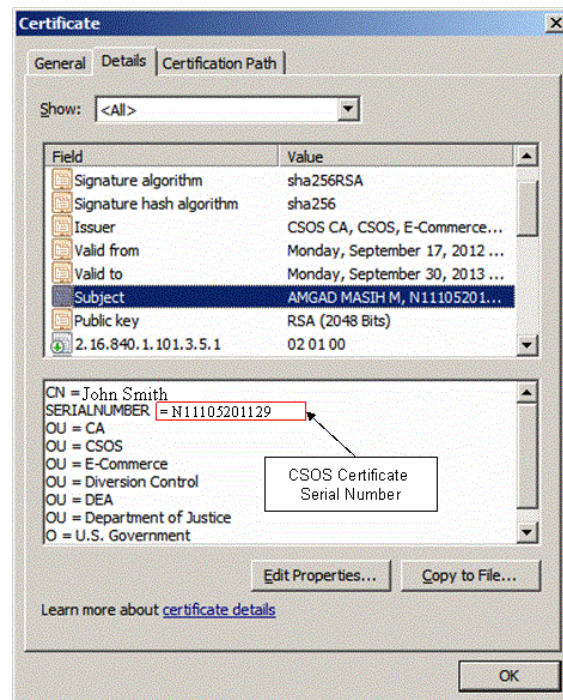


Figure 65: CSOS Certificate Serial Number

Table 7: Hashed DEA Registration Number Value

SHA-2 Hash Value Using	
DEA Registration Number	AA1234567
CSOS Certificate Serial Number	X010122006004
Concatenated DEA Registration Number and CSOS Certificate Serial Number	AA1234567X010122006004
SHA-2 Hash value result using the above concatenated numbers (this is the value appearing in the Certificate)	1b3f544bd58e2145fd771048be40f5b0d89abf2e39ac116313c8e3cc41c3fbb9

The table above provides an example for the inputs and output of the hash value placed in a CSOS Signing Certificate. A Subscriber may verify a Certificate's hash value using software such as a hashing calculator utility. An invalid hash value will result in an error when a supplier attempts to validate a purchase order. Please contact DEA Diversion E-Commerce Support if such an error occurs.

6.0 Certificate Security

The following Certificate Security section refers frequently to the Subscriber's private key. The private key is the component of the subscriber's digital certificate used for digital signatures and therefore is not accessed by anyone (including DEA and suppliers) other than the subscriber.

Passwords or security tokens used to activate the Subscriber private key must never be shared. Methods for protecting the private key and the activation data to that key are discussed in this Certificate Security section. All CSOS Subscribers (e.g., certificate holders) must provide secure storage for their private key. The following sections outline some basic guidelines that help to mitigate the likelihood of a private key compromise

Please note that the Code of Federal Regulations and DEA Diversion Control E-Commerce System Certificate Policy govern the CSOS program. Additionally, the CSOS Subscriber Agreement and Privacy Policy bind all CSOS subscribers. These documents are the official sources for policy regarding the topics mentioned in this section.

6.1 Private keys must be kept private.

If someone other than the Subscriber (owner of the certificate) has access to the private key or password, regulations require that the Subscriber immediately report the compromise (or suspected compromise) to DEA Diversion E-Commerce Support so that the certificate can be revoked. It may be possible for a new certificate to be issued.

6.2 Secure access to the private key.

Use strong passwords or multi-factor authentication to secure access to the private key. The process of digitally signing an order will require the Subscriber to either input a password known only to him or her, or to use a biometrically-activated token (proving that the Subscriber is the private key owner). Passwords used to secure access to the private key must be strong enough so that they cannot be guessed or easily "cracked." Strong passwords include the following characteristics:

- At least 8 characters
- Upper- and lower-case characters
- Numbers and/or special characters, such as the * or # in the middle of the password
- Names or words that *cannot* be found in the dictionary

6.3 Enable the Workstation/PC Inactivity Timeout for 10 minutes.

Once the Subscriber private key has been activated to digitally sign orders, the key must not be left unattended or otherwise available to unauthorized access. Windows PCs using a password-protected screen saver that activates after 10 minutes of inactivity help prevent such unauthorized access if you are away from your desk. Contact your network administrator or DEA Diversion E-Commerce Support for information on this if you are using a Windows Personal Computer (PC).

6.4 Anti-Virus/Spyware Software

Using up-to-date anti-virus/spy ware software helps prevent Trojan horse programs and malicious spy ware, which may “stealthily” install a keyboard logger capable of recording the password and other private information entered into the system. This information can then be transmitted without your knowledge to other parties.

6.5 Backing-up or Escrowing the Private Key

Private Key escrowing involves allowing a third party to maintain a copy of the private key (i.e. the CSOS Certificate). **The CSOS Certificate Policy explicitly prohibits escrowing or backing up of a private key used for digital signatures.**

6.6 Method of Deactivating Private Key

After use, the Subscriber must deactivate the key (e.g., via a manual logout procedure, or automatically after a period of inactivity) so that someone following the Subscriber cannot sign using the key. It is important to completely close (not minimize) the browser window if using a Web-ordering environment to ensure that the activation information is not accessible to others.

6.7 CSOS Application and Auditing Information

DEA does not provide a CSOS software application to organizations for electronic ordering. DEA provides digital certificates for use with approved CSOS enabled software applications. Organizations must develop or purchase CSOS applications that have been audited to DEA regulations by a third party (independent) auditor of the organization’s choosing to ensure that all of the regulations governing the use the electronic orders have been met in the software application. DEA Diversion Investigators may ask an organization to provide evidence of this audit information at any time, and may internally audit an organization’s local enrollment (application) processes to ensure that the processes are maintained as specified in the DEA Diversion Control E-Commerce System Certificate Policy available at www.DEAecom.gov. If you have questions about this auditing or the availability of commercial CSOS applications, please contact DEA Diversion E-Commerce Support. For more information on Auditing, please see Section 7 of this Subscriber Manual or the Code of Federal Regulations available on www.DEAecom.gov.

7.0 CSOS Software Application Audit Requirements

Software applications purchased or developed internally for use with CSOS digital certificates for the purposes of electronically ordering controlled substances must comply with the technical requirements discussed in the 21 CFR, Parts 1305 and 1311. To ensure that the digital signature system functions properly for both the supplier and purchaser, DEA requires that the organization developing the CSOS application software have the application audited by an independent auditor prior to use. If an audited application's order signing or verification processes are modified, those functions of the software application must again be audited to ensure that the application remains in compliance with DEA regulations.

DEA does not require the auditor to submit a copy of the auditing results report to DEA, however application providers must retain a copy of the audit report and submit it to DEA upon request for review. Purchasers of commercial-off-the-shelf (COTS) CSOS applications should request that the vendor provide evidence that the software has been audited and complies with DEA regulations.

8.0 Contact Information

8.1 Support Center Contact Information

E-mail: CSOSsupport@DEAecom.gov

Phone: 1-877-DEA-ECOM

1-877-332-3266

Web: www.DEAecom.gov

A.0 Glossary

Term	Definition
Account Number	The number automatically assigned by the Certificate Authority to each certificate owner
Contact Method	The communication medium used by the customer to submit a support request. Contact methods are typically phone, voicemail, or email.
CSOS Helpdesk	The group responsible for customer support inquiries and requests
CSOS Support	This is the account made publicly available to CSOS subscribers to contact Helpdesk support
Customer	The general term used by the CSOS Helpdesk to describe any person requesting support. Customers include CSOS subscribers as well as non-subscribers.
DEA Number	The customer's registration identification number with the Drug Enforcement Agency that allows for prescription drug transactions. The DEA Number is indicated on the customer's Form 223, and its hashed value is located in each digital certificate.
Organization	A general term used by the Helpdesk to describe the business entity for which a customer is associated
POA	Power of Attorney. A CSOS Customer with order signing authority. See Individual Class.
Renewal	The Registrant Authority process for re-subscribing to CSOS to maintain a valid certificate
Revocation	The disabling of a CSOS certificate.
Revocation Request	The process of submitting a request for the disabling of a CSOS certificate. Revocation requests are approved by the First Registrant
Subscriber	Any individual registered with CSOS, and holding an active certificate
Account Number	The number automatically assigned by the Certificate Authority to each certificate owner

B.0 Acronyms

Acronym	Definition
CA	Certification Authority
CI	Schedule I Controlled Substance
CII	Schedule II Controlled Substance
COTS	Commercial-Off-the-Shelf
CSOS	Controlled Substance Ordering System
DEA	Drug Enforcement Administration
LRA	Local Registration Authority
PC	Personal Computer
PDF	Portable Document Format
PFX	Personal Information Exchange
PKI	Public Key Infrastructure
POA	Power of Attorney
RA	Registration Authority
SHA-2	Secure Hash Algorithm, Version 2
SSN	Social Security Number

C.0 Registrant Attestation

Per Title 21 CFR § 1311.10(a), I confirm that I am the registrant, if an individual; a partner of the registrant, if a partnership; or an officer of the registrant, if a corporation, corporate division, association, trust or other entity.

D.0 Registrant Agreement

I request approval to serve in the role of CSOS Registrant in accordance with the terms and conditions set forth below. By creating this enrollment request, I agree to the terms of this CSOS DEA Registrant Agreement, the CSOS PKI Subscriber Agreement, the DEA Diversion Control E-Commerce PKI Certificate Policy (CP) and DEA Regulation - Title 21, Code of Federal Regulations (1300 to the end).

D.1 Organization Contact for CSOS Registration Authority

I agree to serve as the CSOS Registration Authority point of contact for CSOS Enrollment and CSOS Certificate administration for the DEA Registration(s) identified.

D.2 Distribution of Authorization Codes

I agree to receive from the CSOS Certificate Authority (CA) an authorization code via tamper-proof envelope and secure email, which will be used to activate my digital certificate.

D.3 Certificate Revocation

I agree to request revocation of CSOS Certificates issued with the DEA Registration(s) for which I am responsible if the DEA Registration listed in the CSOS Certificate becomes invalid. The list of events requiring revocation may be found on the CSOS website (www.deaecom.gov) and in DEA Regulation - Title 21, Code of Federal Regulations (1300 to the end).

E.0 Subscriber Agreement

You must read this subscriber agreement before applying for, accepting, or using a DEA digital certificate. If you do not agree to the terms of this subscriber agreement, a certificate will not be issued in your name.

E.1 Terms of Agreement

E.1.1 Representations

THIS SUBSCRIBER AGREEMENT will become effective on the date I create an enrollment request through the CSOS enrollment process.

By creating this enrollment request, I understand that my use and reliance on the CSOS certificate is subject to the terms and conditions set forth below. By SELECTING THE "ACCEPT" OPTION, I (a) agree to be bound by the terms and conditions of this Agreement (Subscriber Agreement), the DEA Diversion Control E-Commerce System Certificate Policy (CP), and the DEA Regulations specified in Title 21, Code of Federal Regulations, (1300 to the end), and (b) represent and warrant to the DEA that the information I provided during the application process is accurate, current, complete and not misleading.

IF THIS AGREEMENT, WHICH INCLUDES THE CERTIFICATE POLICY, IS NOT ACCEPTABLE, THEN THE "DECLINE" OPTION SHOULD BE SELECTED.

E.2 Subscriber Enrollment Procedures

The enrollment process is available through the [CSOS website](#). Please refer to the CSOS Subscriber Manual for a detailed description of Enrollment Procedures. Following enrollment, you will agree to the following:

- a) You will be sent a receipt of enrollment and approval status via email.
- b) Upon approval, you will be mailed a one-time access code in a tamper-evident envelope. This envelope must not have been opened prior to your receipt. You will receive a password via your email account that you provided on the application form. Do not share your access code or password with anyone.
- c) Upon receipt of both the access code and password, please download your CSOS CA certificates. You will find the instructions to obtain the certificates in [the CSOS Subscriber Manual](#).

E.3 Identification Information Attestation

When submitting identification information:

- a) I agree that any information I submit is accurate, current, complete and not misleading.
- b) I agree that I will immediately inform the DEA if any information changes submitted during the application process.

E.4 Obligations

The DEA may revoke the Subscriber's certificate(s) at any time upon failure to meet any of the terms of this agreement. Subscriber obligations are detailed below.

E.4.1 Certificate Review

The DEA will notify you and your CSOS Coordinator when your certificate is ready for retrieval. After downloading your certificate, you agree to review and verify the accuracy of the information contained in your certificate, and to immediately notify the DEA of any inaccuracies.

E.4.2 Certificate Protection

All Subscribers are obligated to:

- a) Protect the private signing key. A certificate holder must not share the private key with any other individual.
- b) Protect the password. A certificate holder must not share the password with any other individual.
- c) Request a certificate revocation using the CSOS Web Application in the event of a suspected compromise of the private signing key, password, or event requiring key revocation.

The list of events requiring revocation may be found on the CSOS website (www.deacom.gov) and in DEA Regulation - Title 21, Code of Federal Regulations (1300 to the end). Once a certificate is revoked, you must request a new certificate.

E.5 Acceptable Use

CSOS Certificate usage is restricted to CSOS activities.

E.6 Subscriber Account Management

Once enrolled, you must update any personal information that changes in the CSOS Web Application within 60 days of the change.

E.7 Certificate Expiration

The CSOS certificate shall expire upon the expiration of the DEA Registration.

E.8 Terms of Agreement

This Agreement constitutes a renewable contract whose duration aligns with the DEA Registration expiration date. The contract may be terminated (i) by you at any time, or (ii) by the DEA at any time with notice to the Subscriber.

E.8.1 General

You understand and agree that if any provision of this Agreement is declared by a court to be invalid, illegal, or unenforceable, all other provisions shall remain in full force and effect.

E.8.2 Availability

You understand that the Certificate Revocation Lists (CRL) are available 7 days a week, 24 hours per day in accordance with the policies and processes described in the CP for certificate verification. Note this is not a warranty of 100% availability. Availability may be affected by system maintenance, system repair, or by factors outside the control of the CA.

E.8.3 Requests

Requests for the certificate issuance, renewal, and revocation shall be processed within the CSOS application.

Assistance may be requested via phone to the CSOS Helpdesk at 1-877- DEA-ECOM (1-877-332-3266) toll-free.

E.8.4 Dispute Resolution and Governing Law

This Agreement shall be governed by and construed in accordance with the laws of the United States of America.

E.8.5 Extraordinary Events

The DEA will incur no liability, costs, damages or loss if circumstances beyond its control (such as, but not limited to, fire, flood, delay in the U.S. mail or interference from an outside force) prevent proper execution of any CSOS transactions.

E.8.6 Privacy Notification

See the DOJ Privacy Policy. (<https://www.justice.gov/doj/privacy-policy>)

E.8.7 Additional Resources

The following documents may be obtained by going to <http://www.DEAdiversion.usdoj.gov/>

- DEA Diversion Control E-Commerce System Certificate Policy (CP)
- DEA Regulations - Title 21, Code o