

EPCS Token: Prescriber's Tasks

The purpose of this document is to help guide the prescriber through the process of setting up their EPCS Token which is needed for prescribing controlled substances.

This is a three-step process that will require the prescriber to:

- 1) Apply for a certificate which requires you to have an iPhone or Android
- 2) Verification which you will need to wait for 24-48h
- 3) Install certificates on a computer which helps authorize user with IdenTrust. Consideration should be given as to which computer should be used for this step. Backing up of these certificates is important.

**** As you are prompted to create a username, email and/or password (s), we recommend that you use the same values throughout the process.**

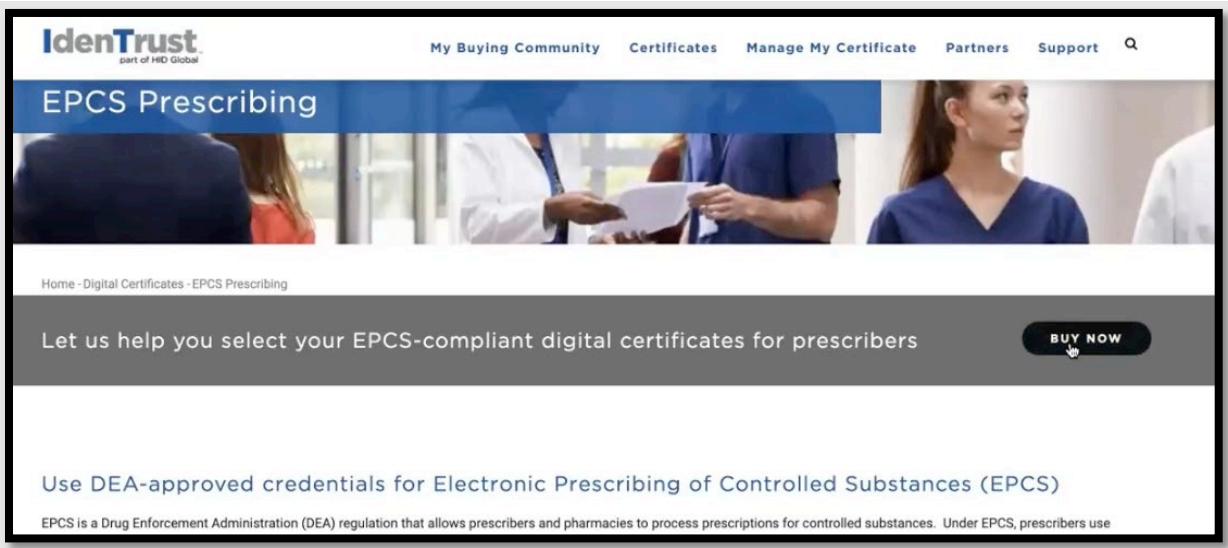
Step 1 (Time to complete: 5 minutes; Location: any device)

Obtain IdenTrust Voucher

1. Depending on how your county has set up this part, you will receive a voucher with a unique # by email from your county medical director or county point person.
2. Open any browser to: <https://www.identrust.com/certificates/epcs-prescribers>
3. Select EPCS Prescribing from the Certificates tab



4. Scroll down and select blue "Buy Now" button. *You will not be purchasing any items.*



5. Scroll all the way down and enter your unique Voucher #

The screenshot shows the IdenTrust website interface. At the top, the IdenTrust logo is on the left, and navigation links for "My Buying Community", "Certificates", "Manage My Certificate", and "Support" are on the right. Below the navigation, there are radio button options for "StreamlineMD, A PRC Medical Company", "Vendor Program Is Not Listed", "WEBeDoctor", and "Wellsky". A blue "NEXT" button is positioned below these options. A red rectangular box highlights a form field with the text "If you have a Voucher Number please enter it here:" followed by an empty input box and a blue "SUBMIT" button. Below this, there is a "LOG IN" button and a link to "Use the Certificate Management Center to renew an existing certificate".

6. This will take you to "Apply for the IGC Basic Assurance | Individual Identity | Software Storage | Mobile Authentication Certificate". Your voucher # should have pulled over, but if not, please re-enter and for program affiliation select "Streamline Healthcare Solutions"

The screenshot displays the "Apply for your IGC Basic Assurance | Individual Identity | Software Storage | Mobile Authentication Certificate" page. The page title is prominently displayed at the top. Below the title, a paragraph explains that the certificate is a form of identification used within the IdenTrust Global Common Certificates Program and lists the steps to complete: 1. Apply, 2. Get Verified, and 3. Retrieve Your Certificate. Each step includes a brief description and a question mark icon for help. Below the steps, there is a section for "Voucher, if you have one" with a "Voucher Number" input field. Underneath, it shows "Hardware Type Selected" as "Browser \$0.00". A paragraph instructs the user to select the program where the certificate will be primarily used. A dropdown menu for "*Program Affiliation*" is shown with "STREAMLINE HEALTHCARE SOLUTIONS" selected. At the bottom, there are "CANCEL" and "NEXT" buttons.

1. In the "Your Information" page, fill out the information as requested. *(For those with vouchers, the credit card info is just for verification and is NOT used for any payment)*
2. Please create a **username (email) and password that you will use throughout this set-up and to store it securely.** For some counties, they will be asking you to share back your username and password in case of recovery so please pick a password that is not commonly used for your other personal password.
3. A pop-up should appear asking for you to confirm your information. Click confirm if accurate.
4. A Subscriber Agreement will appear and click that you have read and accepted the terms. Click. 'Submit Application'
1. Your application should now be submitted, and you will be greeted with this screen indicating so. **Be sure to verify your email address as they will send the information necessary for next steps to the email registered to the account.**
2. Click the Finish button to proceed. Please be sure to close your browser windows to complete the next steps.

Step 2 (24-48 hours waiting period)

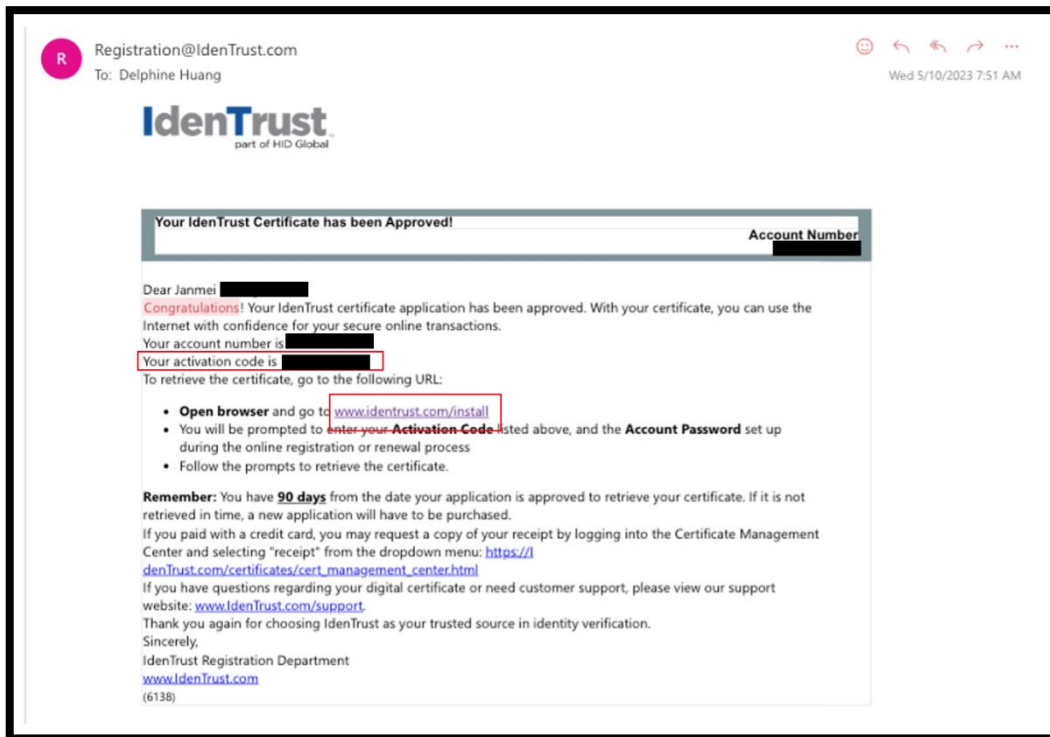
Verification Period

1. 24-48 hours to complete the verification. You will receive an email from IdenTrust stating that you have been approved and will provide an activation code. If you do not receive a notification, A) check your spam or local IT to check the spam filter B) Please contact Chris.Watson@calmhsa.org

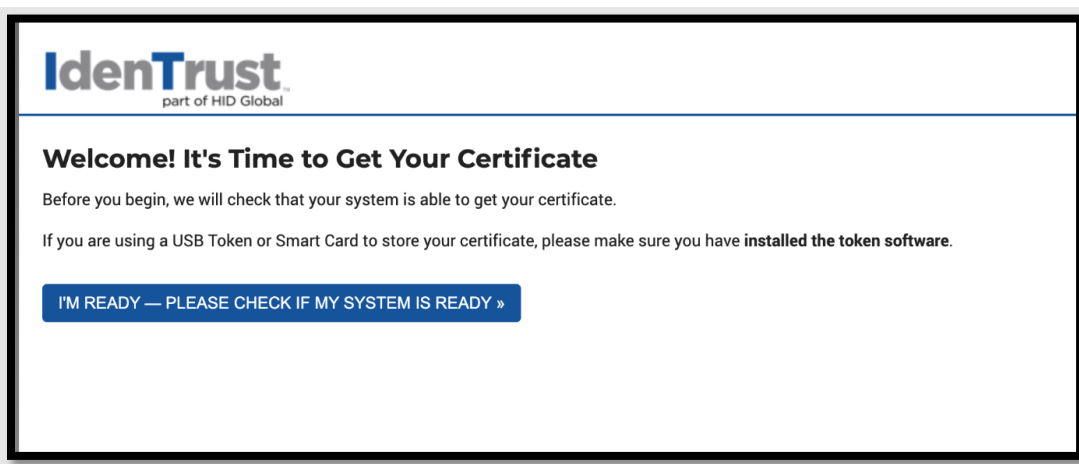
Step 3A (10 minutes, Location: county/clinic computer and mobile device required)

Certificate Retrieval

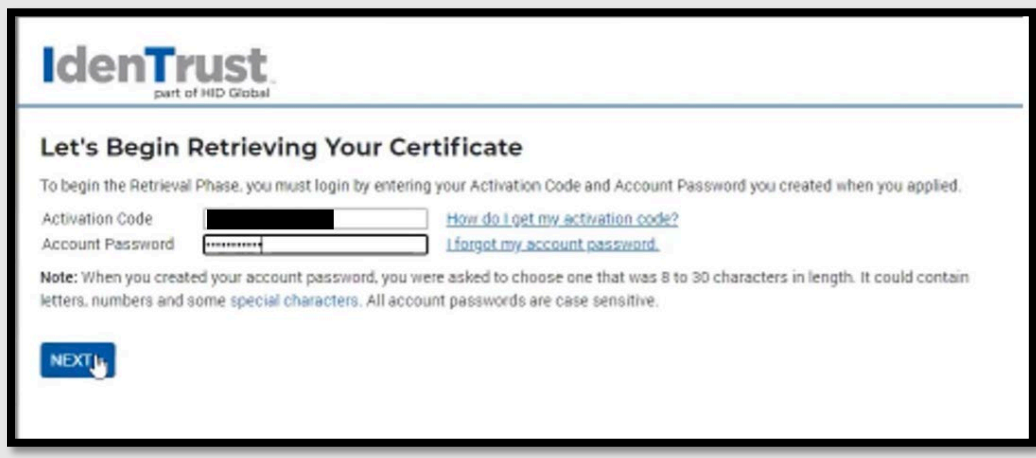
1. At a county or clinic designated computer, open your verification email, click on the link supplied in the email to retrieve your certificate. The activation code from the email and the password set during the application process will be used to obtain the digital certificate.



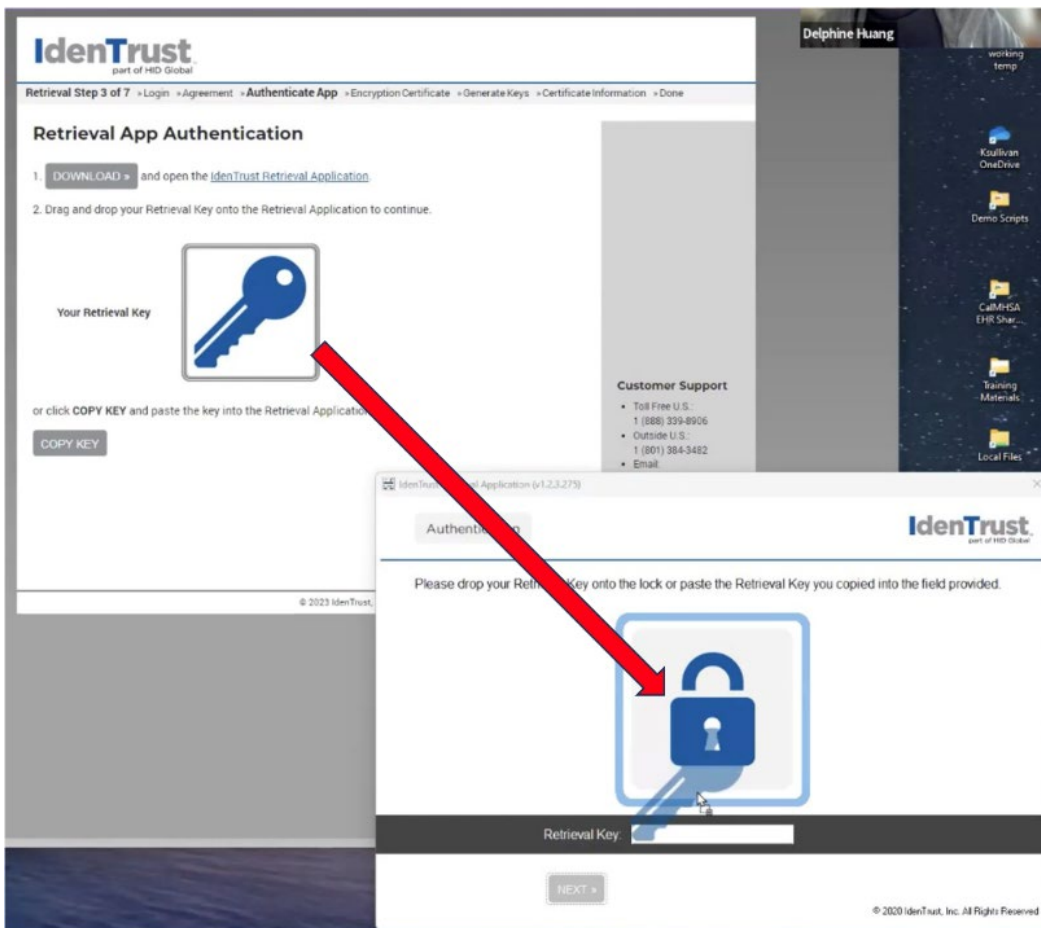
2. Next, click on the "I'm Ready..." button



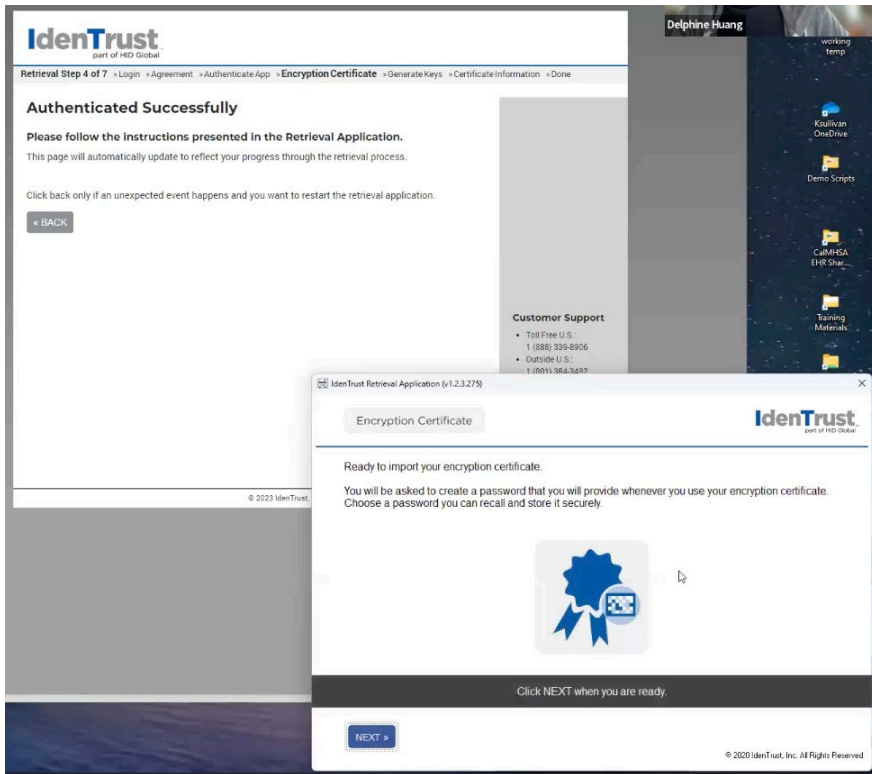
3. Add your activation code and use your Account Password



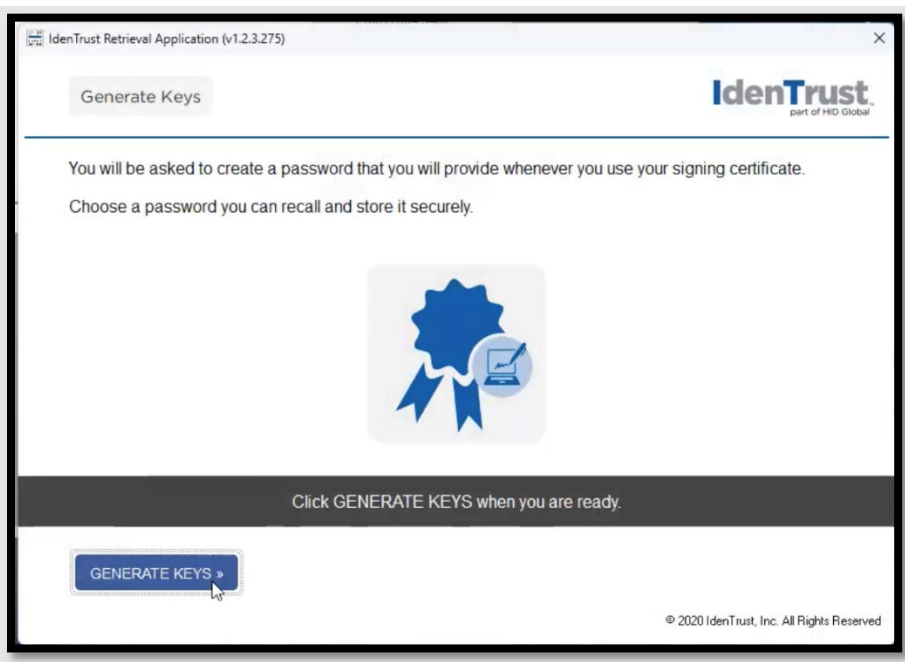
4. Click the blue "Download" button to start the Retrieval Process. Open the IdenTrust Retrieval App on your computer.
5. A pop up with a lock will appear. Drag the key image to the padlock image shown in the application to unlock the certificate. (If this does not work, try clicking Copy Key and paste it in the Retrieval Key field in the application)



6. If the key was retrieved successfully, you will be notified with the next screen titled "Authenticated Successfully".
7. Next, you will need to import your encryption certificate.

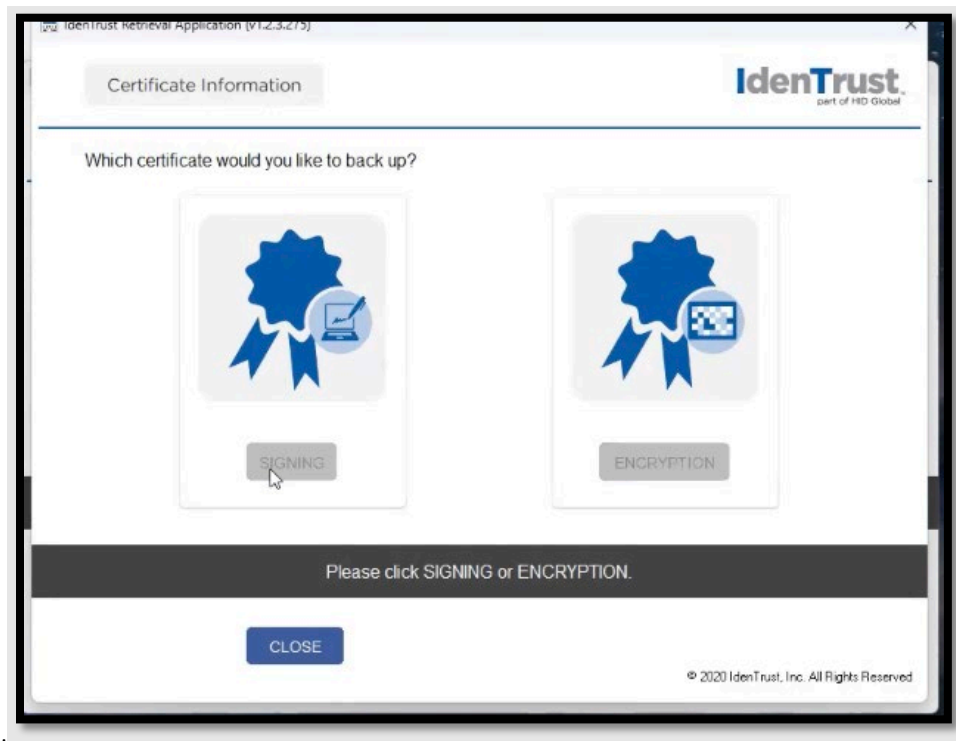


8. You will be prompted to choose security level, please select “High” and create a new password and confirm password. Choose, ‘OK.’ If your computer alerts a security warning, please select “Yes”
9. You will be asked to “Generate Keys,” and if prompted to select security level, enter “High” and create a new password and confirm password. This will generate a public/private key pair and you will notified you when in the installation is successful.



10. It then will go through an install process including ‘Install full certificate chain.’

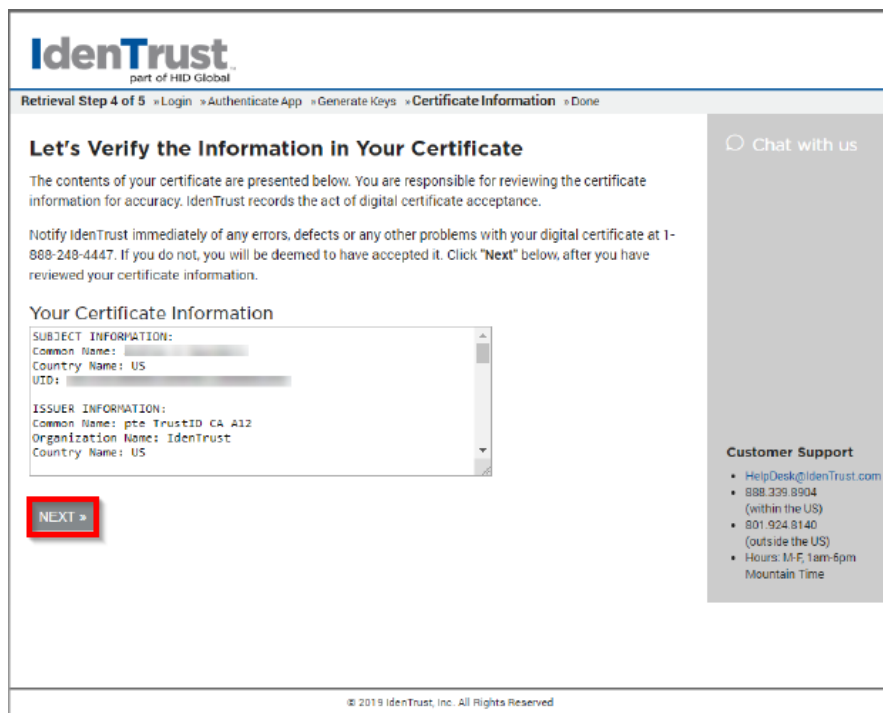
11. We recommend that you back up the Signing and Encryption certificates and save your account password in a secure location. Some counties may require that you send this information to your county medical director or county point person. Remember that you will need these certificates and information in order to authenticate yourself with IdenTrust.



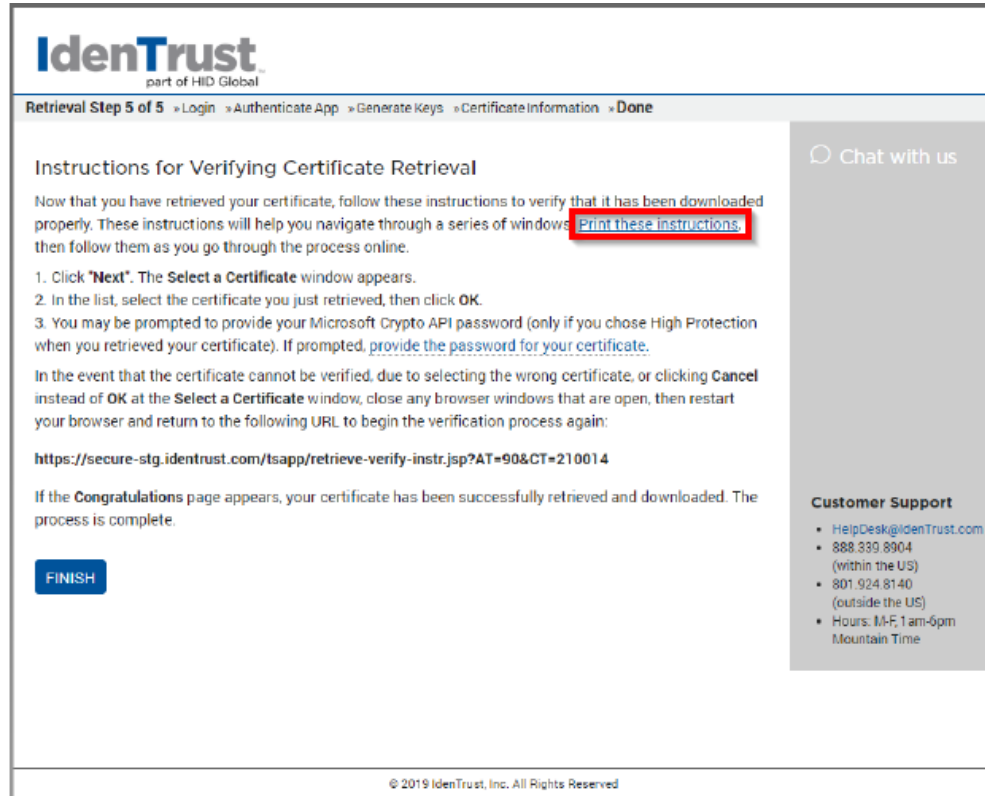
12. At this point you can either click 'See My Cert' to display the details of the certificate, or 'Test My Cert' which will validate your certificate online via the internet. (We recommend clicking 'See My Cert' to verify the information is correct.)



13. Once 'See My Cert' is clicked this screen will appear. Verify the information is correct and then click 'Next.'



14. The user should now see this screen appear. Select the Print these Instructions link and follow them as you go through the process.



Once done, please close all instances of your browser to continue with the next steps of the certificate process.

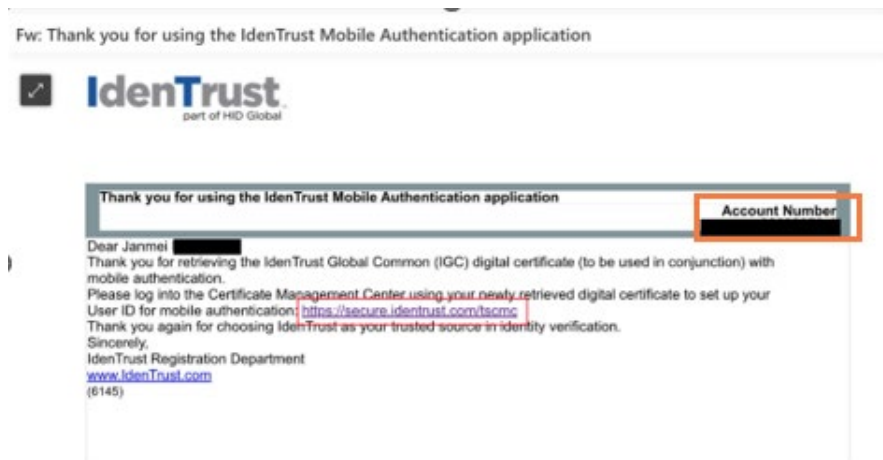
Step 3B (10 minutes, Location: county/clinic computer and mobile device required)

Pair your mobile device

1. An email will be sent to the registered email address containing instructions and a link. From the computer that the certificate was installed on, access the IdenTrust Certificate Management Center via the link in the email or by the following URL:
<https://secure.identrust.com/tscmcapp/>
 - a. When prompted, provide the certificate as the authenticator. It should popup for you to choose. (This must be done on the system that the certificate was installed on or it won't work.) The certificate acts as the authenticating mechanism to get you into the Certificate Management Center.

If this step worked for you and you were able to get into the Certificate Management Center, proceed to step 2. If it doesn't work for you, follow the next steps for the other way to get into the website. If the certificate method didn't work, you should contact CalMHSa for assistance as it should work.

NOTE: If the certificate doesn't pop up or you aren't on the computer that has the certificate installed, you still can access the website to continue the process. You will need the account number (which would have shown in one of the emails, and the account password you created.)



Login using your Account number (Top right corner of the email) and your Account Password

IdenTrust
part of HID Global

Certificate Management Center

Login

To access, you may [present a valid certificate](#) or enter your account number and account password.

Account Number [How do I get my account number?](#)

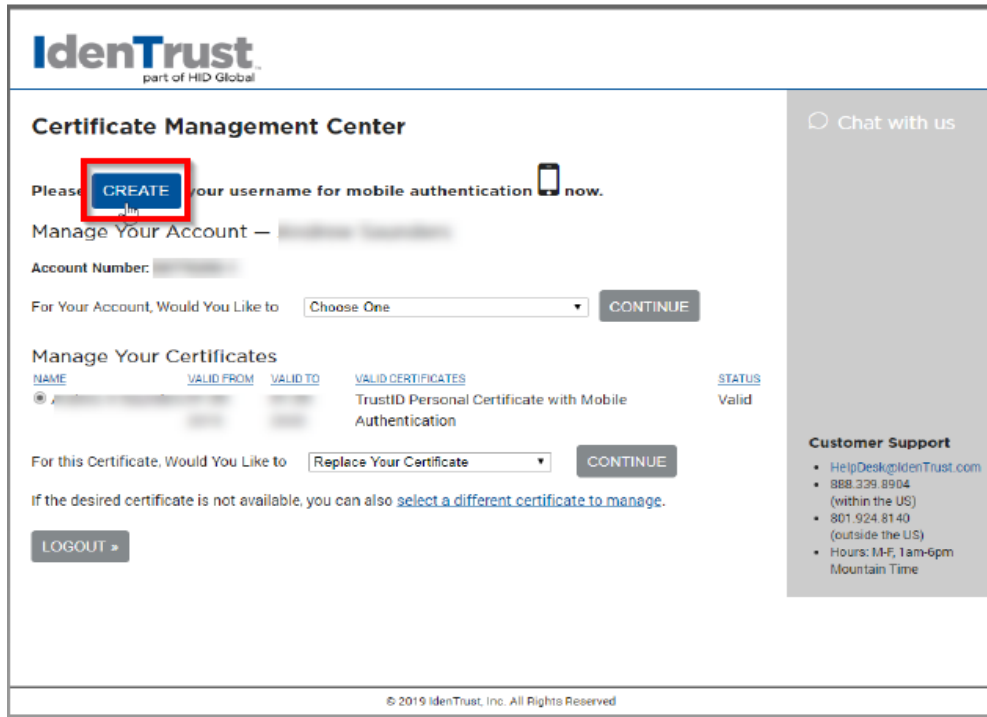
Account Password [I forgot my account password.](#)

Note: Your Account Password is 8-30 characters in length and may contain letters, numbers and [some special characters](#), and is case sensitive.

LOGIN »

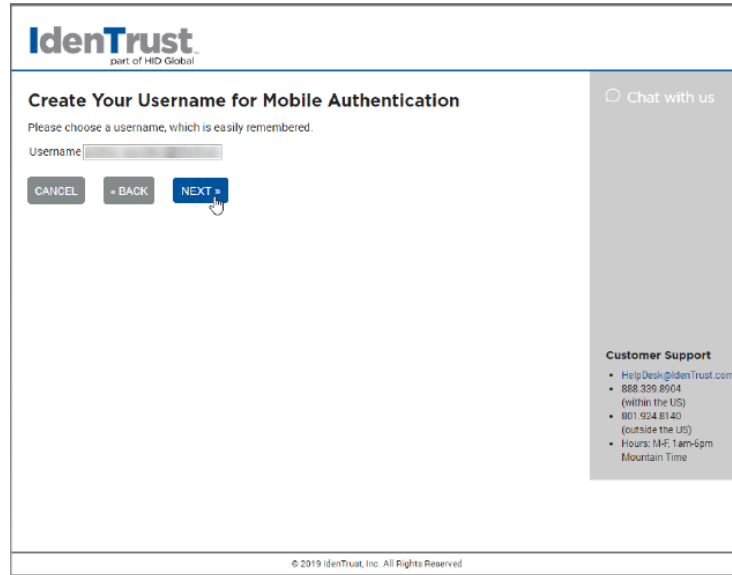
2. The system should prompt you to create a Mobile Authentication username.

Select the 'Create' blue icon to create the username. The system will recommend using the registered email address to use as the username (we recommend using your work/county email address). Please keep note of this mobile device username as it will be used to link your device to Rx in Smartcare.



NOTE: If the icon is greyed out or you need to redo the username you can go to the option: **For Your Account Would You Like to:** Select the dropdown and choose 'Create Your Authentication Username.'

3. Click 'Next' once the username is verified as unique.

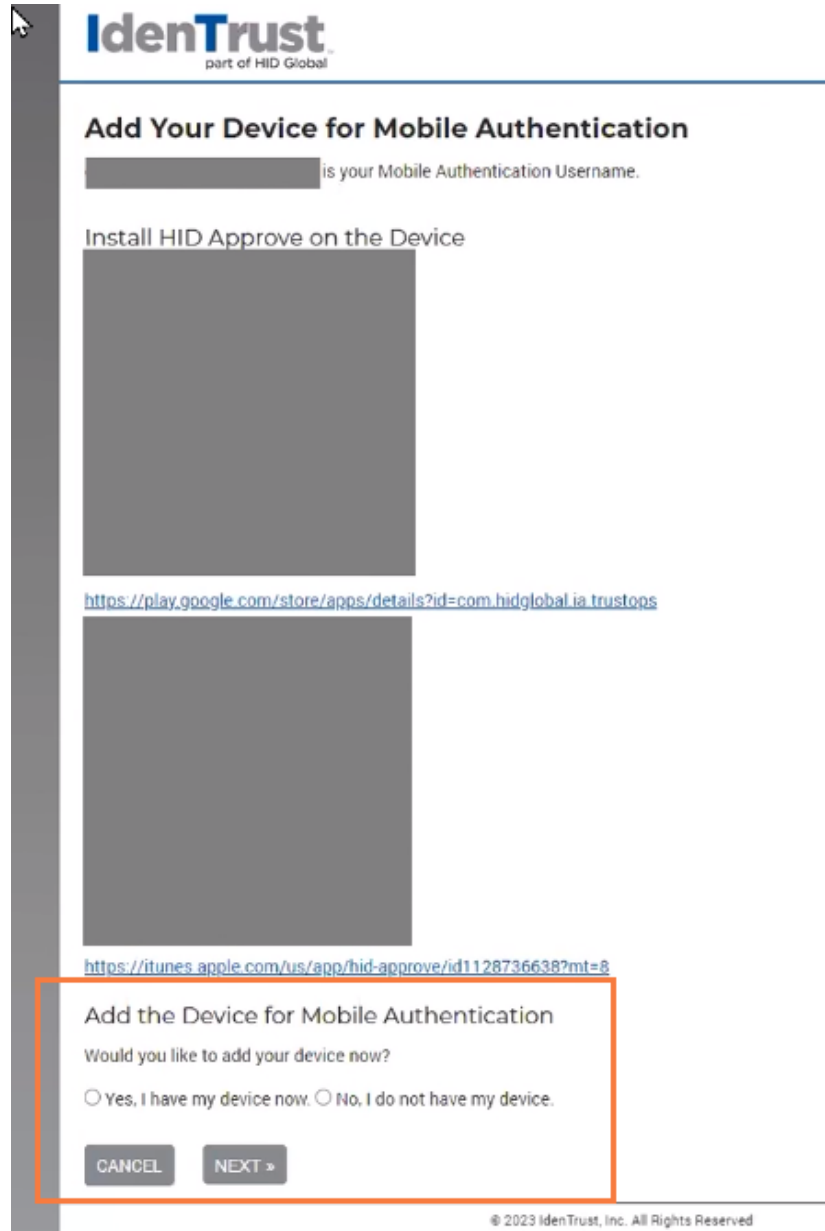


The screenshot shows a web page for IdemTrust, a part of HID Global. The main heading is "Create Your Username for Mobile Authentication". Below this, there is a prompt: "Please choose a username, which is easily remembered." A text input field labeled "Username:" is present, with a greyed-out placeholder. Below the input field are three buttons: "CANCEL", "BACK", and "NEXT". A mouse cursor is hovering over the "NEXT" button. On the right side of the page, there is a "Chat with us" link and a "Customer Support" section with the following details:

- HelpDesk@IdemTrust.com
- 888.339.8604 (within the US)
- 801.924.8140 (outside the US)
- Hours: M-F, 1am-5pm Mountain Time

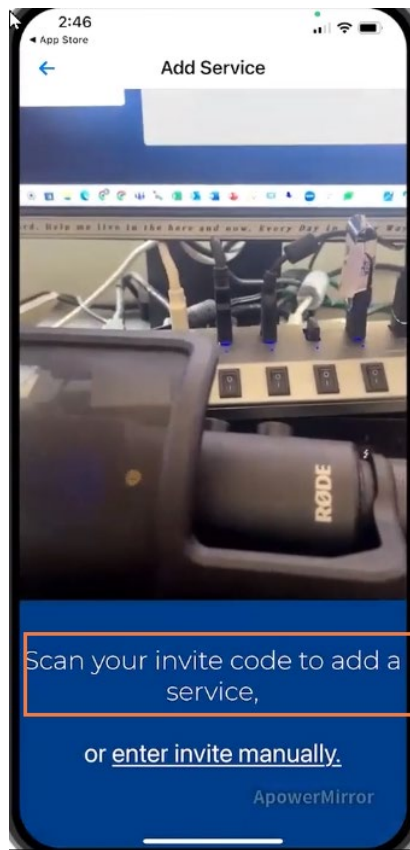
At the bottom of the page, there is a copyright notice: "© 2019 IdemTrust, Inc. All Rights Reserved".

3. At this point you will be prompted to install the 'HID Approve' app onto your mobile device. You can either use the QR codes and scan them with your phone's camera to be taken to the app store to download the app, or just search HID Approve in your phone's app store.
 - a. **Install app using QR code or through app store.** (NOTE: QR Codes are greyed out sections below.)
 - b. Once the app is installed, **select the radio button next to 'Yes, I have my device now'** and **select 'Next.'**

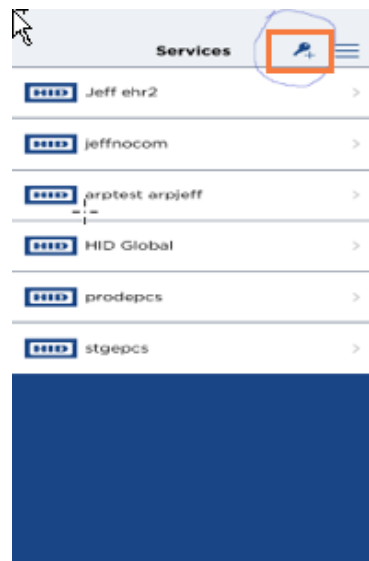


4. Once installed, the next step is to link your phone to the certificate/IdenTrust either via the QR code or manual entry.

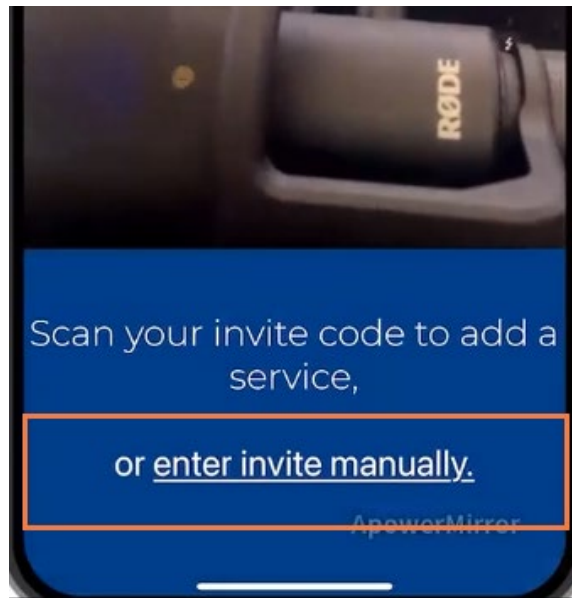
5. Open HID Approve app on your phone. You will be prompted to scan the QR code or enter it manually.




If not prompted, scan the QR Code on your computer screen using the 'key' button at top right of the screen in the HID app. (This could take a couple of attempts to get the scan to work.)



NOTE: If this doesn't work, select the 'enter invite manually' link in the app and enter the information in their corresponding fields.



Manual entry items (user information on your computer screen, not information from the screenshot.)



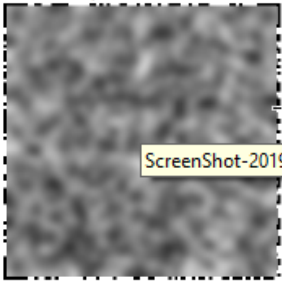
Add Your Device for Mobile Authentication

On your mobile device, please install HID Approve.

Android <https://play.google.com/store/apps/details?id=com.hidglobal.ia.trustops>
iOS <https://itunes.apple.com/us/app/hid-approve/id1128736638?mt=8>

Scan the QR code

1. Download the HID Approve app to your mobile device.
2. Launch HID Approve
3. Scan the QR code



Or optionally, Manually Register

Use HID Approve to add a new service.

- Username: [redacted]
- Invite Code: [redacted]
- Service URL: **preprod.aaas.hidcloud.com:443/tf0ed5520b236937308730**

FINISH »

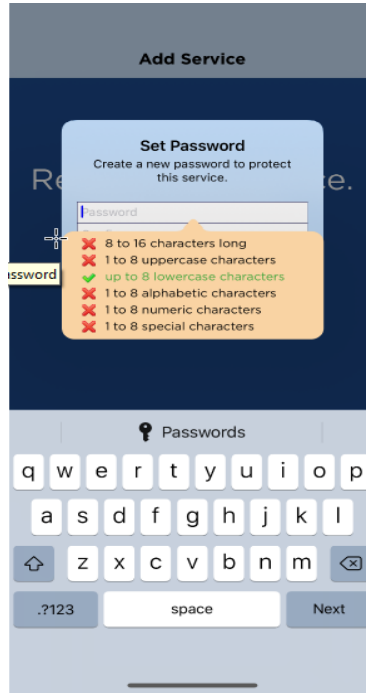
© 2019 IdenTrust, Inc. All Rights Reserved

Chat with us

Customer Support

- HelpDesk@IdeaTrust.com
- 888.339.8904 (within the US)
- 801.924.8140 (outside the US)
- Hours: M-F, 1am-6pm Mountain Time

- Once the certificate and IdenTrust are linked to your mobile device, you will be prompted to set a password in the HID Approve app.



- You will be prompted to register and create a password on your phone. You will receive a notification that your HID Global Service has been registered successfully. Your certificate is now linked to your device. Click FINISH on the computer.

Test your mobile device

1. To test the device, logged into the Certificate Management Center screen and select “Test Your Authentication Device” from the first dropdown and click CONTINUE.

The screenshot shows the IdenTrust Certificate Management Center interface. At the top, it says "IdenTrust part of HID Global". Below that is the title "Certificate Management Center" and "Manage Your Account — Janmei [redacted]". The account number is [redacted]. The mobile authentication username is [redacted]@calmhsa.org. There is a dropdown menu with "Test Your Authentication Device" selected and a "CONTINUE" button. Below this is a section "Manage Your Certificates" with a table of certificates. The table has columns for NAME, VALID FROM, VALID TO, VALID CERTIFICATES, and STATUS. One certificate is listed: Janmei [redacted], valid from 05-12-2023 to 05-11-2025, with valid certificates "IGC Basic Assurance | Individual Identity | Software Storage | Mobile Authentication Certificate" and a status of "Valid". Below the table is another dropdown menu with "Replace Your Certificate" selected and a "CONTINUE" button. At the bottom, there is a "LOGOUT >" button.

2. Follow the presented prompt to select your authenticated phone, and a test request should be sent to the mobile device. Confirm the request by swiping the green APPROVE option. You will be prompted to enter your password and you will be notified if the test was validated. You will be notified by email that your mobile device was added.

The image shows two screenshots of the mobile authentication process. The left screenshot is a desktop view of the "Test Your Mobile Authentication Device" screen. It says "Please select the device to test." and has a dropdown menu with "iPhone" selected. There are "CANCEL", "+ BACK", and "NEXT >" buttons. The right screenshot is a mobile phone screen showing a "HID" logo at the top. Below it is a white box with the text "Enter Password" and "Enter the password protecting this service." There is a password input field with a toggle for visibility. Below the input field are "Cancel" and "OK" buttons. At the bottom of the screen, there is a green "Approve >" button and a red "Decline <" button. The text "authenticate request" is visible at the bottom of the screen.

- Contact your county medical director or point person to let them know that you are ready for Surescript and EPCS within the EHR.
- Now, you are set up for go-live. More instructions will be sent to you 1 week before.