



Patriot Act Communication System



Supervisory User Enrollment Guide Version 1.2

Version released: 5/27/2003



Introduction

As discussed in the 'Getting Started' section of the PACS public website, the Supervisory User serves as a liaison between PACS and his/her filing institution. Supervisory User enrollment is therefore the first step in creating the relationship between PACS and your filing institution. It is important to note that only the initial Supervisory User from each filing institution should complete this process. All other users from the filing institution, including any back-up Supervisory Users, will enroll via a distinctly different process.

There are five basic steps involved in enrolling as a Supervisory User, as follows:

1. Downloading the PureEdge Forms Viewer
2. Applying for a Supervisory User Digital Certificate
3. Communicating with the Supervisory User authorizer
4. Downloading the Digital Certificate
5. Enrolling in PACS

If you are reading this guide you have decided, based on the information presented on the *Should I Use PACS?* section of the public website, that it is appropriate for you to enroll as the initial Supervisory User for your filing institution. You should continue through this enrollment guide completing the steps in sequence. Questions or issues encountered during the Supervisory User enrollment process may be directed to the **PACS Help Desk** at 1-888-827-2778 (select option 6) or via e-mail at PACSHelp@notes.tcs.treas.gov.

Throughout this guide you will occasionally see shaded text boxes containing bold and italicized text such as the one below. Pay special attention to the information in these boxes as it is critical to your successful enrollment in PACS.

Note: This is a one-time use guide meant only for the initial Supervisory User from each filing institution. After you have completed the steps contained herein this guide may be discarded and will not be needed by any subsequent enrollees or for any other actions performed within PACS. Other responsibilities that are specific to Supervisory Users (e.g., initiating the enrollment of other users, managing filing institution information, tracking the status of the institution's filings) are discussed in the Supervisory User Manual which will be available once you have successfully enrolled.



1. Downloading the PureEdge Forms Viewer

The PureEdge Forms Viewer is available for download from the PACS public website (<http://pacs.treas.gov>). It allows you to view and prepare electronic CTR and SAR forms on PACS, view PACS Alerts, create Secure Messages to send to FinCEN, and submit digital certificate requests. The PureEdge application requires approximately 4,039 kilobytes free space on your hard drive.

Note: *If you are not able to download executable files due to your institution's firewall and/or downloading policies, contact the PACS Help Desk at 1-888-827-2778 (option #6) or PACSHelp@notes.tcs.treas.gov for assistance.*

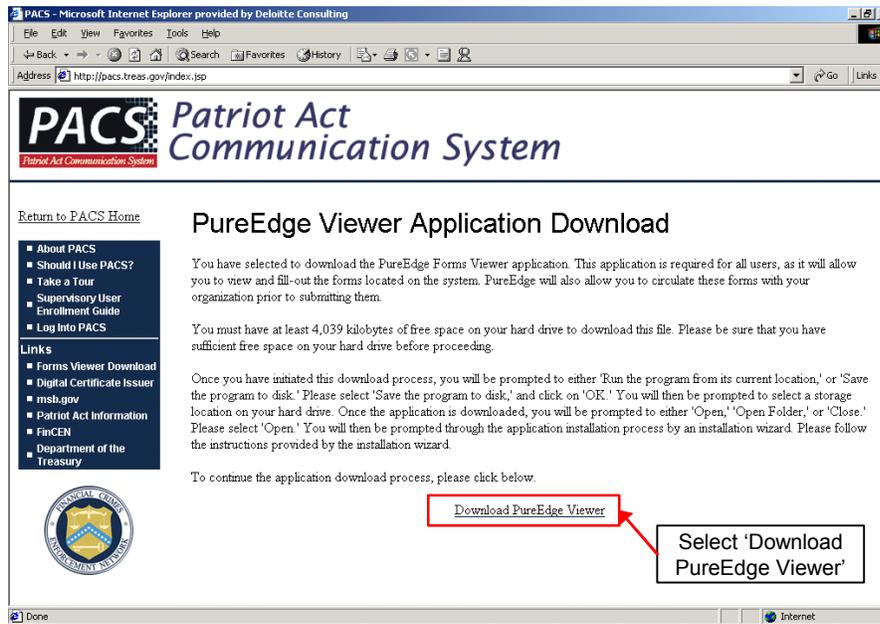
The steps required to download the PureEdge Forms Viewer are as follows:

1. Access the PACS public website at <http://pacs.treas.gov>.
2. Click on the **Forms Viewer Download** link located on the left navigation bar of the PACS site (shown in the following graphic).

The screenshot shows the PACS homepage in a Microsoft Internet Explorer browser window. The address bar shows <http://pacs.treas.gov/index.jsp>. The page title is "ACS Patriot Act Communication System". The main content area says "Welcome to the PACS Homepage" and provides information about the system. On the left, there is a navigation menu with a "Links" section. A callout box with the text "Select the Forms Viewer Download option here." points to the "Forms Viewer Download" link in the "Links" section. Other links in the "Links" section include "Digital Certificate Issuer", "mstl.gov", "Patriot Act Information", "FinCEN", and "Department of the Treasury".



3. Review the PureEdge Viewer Application Download instructional page and click the **Download PureEdge Viewer** link.



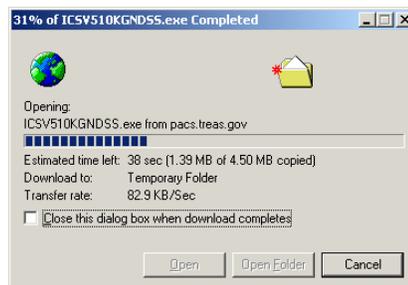
4. Select the **'Run this program from its current location'** option on the pop-up window and click the **OK** button.



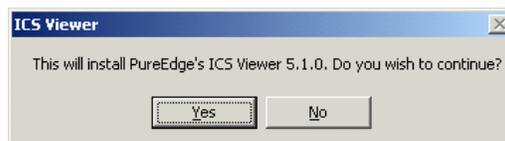


5. Wait while the PureEdge installation files are transferred to your computer. This may take a couple of minutes, even with a high-speed Internet connection.

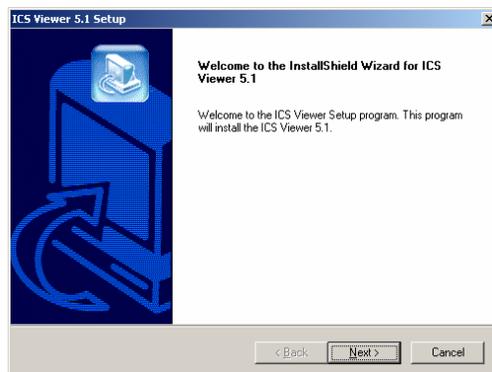
If presented with a security warning asking if you want to install and run “ICS Viewer”, click **Yes**.



6. Click **Yes** when prompted to install the PureEdge Viewer.



7. Follow the InstallShield Wizard prompts to complete the PureEdge installation process. Accept the default options presented to you on all screens as you proceed through the InstallShield Wizard. The PureEdge InstallShield Wizard will present a message when the installation is complete. On the last screen you should uncheck the ‘**Launch the application**’ checkbox and then click **Finish**.





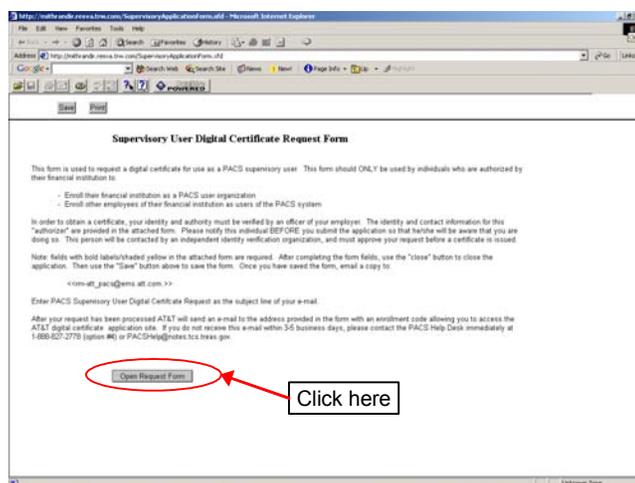
2. Applying for a Supervisory User Digital Certificate

Digital certificates are required to access the secure portion of PACS, where the electronic filing and messaging capabilities exist. They are required because they protect information by:

- Authenticating users involved in electronic transactions (providing technical non-repudiation),
- Ensuring that electronic messages have not been altered or corrupted during electronic transfer, and
- Protecting information from interception during electronic transmission.

Digital certificates for PACS are provided by a certificate vendor associated with the U.S. Government's ACES digital certificate program. A Supervisory User digital certificate will provide you with Supervisory User access to PACS. The procedure for applying for a Supervisory User digital certificate is as follows:

1. Access the PACS public website at <http://pacs.treas.gov>, select the **Should I Use PACS?** link from the left navigation bar, and select the **Getting Started** link that appears at the very bottom of this page.
2. There are five questions at the top of the *Getting Started* page. Click on the fourth question, "*I am the Supervisory User for my institution. What do I do next?*"
3. Click on the **Supervisory User Digital Certificate Request Form** link contained in the paragraph titled, "*Step 1: Enroll Yourself and Your Filing Institution.*"
4. PACS will display the cover page of the *Supervisory User Digital Certificate Request Form*, which contains instructions for completing and submitting the form. Should you need to open a previously saved form use the **Open Form** button () located on the form's toolbar. Click on the **Open Request Form** button to open the portion of the form where you will enter your request information.



5. Each section of the *Supervisory User Digital Certificate Request Form* contains instructions for completing the form correctly. Please be sure to read all instructions contained on the form. You may save your form at any point by selecting the **Save** button at which time you will be prompted to select the exact location on your computer where you want to save the form. (**Note: The form is saved on your computer, not on PACS.**)



6. In the first section of the form, *Supervisory User Personal Information*, enter the requested information about yourself (required fields have bold labels and are shaded yellow). Please be sure that you enter your correct e-mail address as it will be vetted by a third party organization and used to distribute enrollment codes for both you and your back-up Supervisory User (the same e-mail address should be used throughout the entire enrollment process). Supervisory User personal information includes the following:

- Title
- First Name
- Middle Initial
- Last Name
- Job Title
- Phone Number
- E-mail Address
- Business Name
- Business Address

7. In the second section of the form, *Backup Supervisory User Personal Information*, enter equivalent information for your back-up Supervisory User. **Note: If you choose to enter information for a back-up Supervisory User, you must enter the same information that is required for the first Supervisory User.**

8. In the third section of the form, *Authorizer Information*, enter the information relating to your business and the individual who will authorize you as a PACS Supervisory User (required fields have bold labels and are shaded yellow). As the form suggests, be sure the authorizer you enter has the appropriate authority within your institution to confirm you as the initial Supervisory User. Also be sure the authorizer's contact information is accurate because it will be vetted by a third party organization. Authorizer information includes the following:

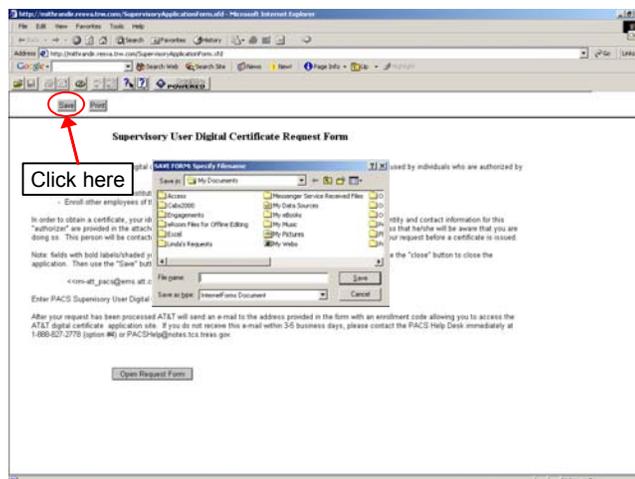
- Title
- First Name
- Middle Initial
- Last Name
- Authorizer Phone Number
- Authorizer E-mail Address
- Common Business Name
- Formal (Legal) Business Name
- Business Address
- Business City
- Business State
- Business Zip Code
- Business Country
- Business Phone Number
- DUNS Number
- Group or Department

If your institution has fewer than 25 employees then your authorizer may be the same as the Supervisory User or back-up Supervisory User. If this is the case, please select the checkbox in this section of the form.

9. After verifying that you have entered accurate information, click the **Close** button at the top of the form to return to the form's cover page.



- Once you have returned to the cover page you should save the form if you have not already done so. To save the form click the **Save** button and select the exact location on your computer where you would like the form to be saved. (**Note: The form is saved on your computer, not on PACS.**) Remember where on your computer you are saving this form as you will need to access it in the next step.



- In order to submit your request to the ACES program vendor you must e-mail (using your own e-mail system) this form as an attachment to: rm-att_pacs@ems.att.com. Enter 'PACS Supervisory User Digital Certificate Request' as the e-mail subject and leave the body of the message blank.

The ACES program vendor will notify you via e-mail when the vetting process is complete and will provide you with unique **Enrollment Codes** (labeled as Pre-Authorized Numbers in the notification e-mail) for both yourself and your back-up Supervisory User if applicable. The notification e-mail will come directly from the ACES program vendor (i.e., username@att.com). Only you, as the Supervisory User, will receive this e-mail. It will be your responsibility to provide the back-up Supervisory User with the required information after you have enrolled yourself (see the end of Section 5 in this guide for more detail regarding information to provide to the back-up Supervisory User).

Once you receive this notification from the ACES program vendor, continue with Section 4, *Downloading the Digital Certificate*, of this guide. In the meantime, you should contact your authorizer as discussed in Section 3, *Communicating with the Supervisory User Authorizer*.

Note: You should receive e-mail notification from the ACES program vendor within 3 to 5 business days after submitting your application. If you have not received any communication (certificate approval or rejection) from the ACES program vendor within 5 business days, please contact the PACS Help Desk immediately at 1-888-827-2778 and select option 6.



3. Communicating with the Supervisory User Authorizer

After you have completed and submitted your digital certificate request to the ACES program vendor they will pass your information to a third party organization that will vet your identity and your designation as a PACS Supervisory User. In order to complete this vetting process, the third party organization will verify the authorizer's business location and contact this person by telephone.

The third party organization will be asking the authorizer a short series of questions regarding your employment status at the filing institution, your authority to assume the Supervisory User role, and the accuracy of the personal information you entered in the request form. The third party organization will ask the authorizer the same questions regarding the backup Supervisory User, if you selected one. If you are to be an official Supervisory User for your institution, it is critical that the authorizer answer these questions positively. If your authorizer cannot confirm the information you submitted, your request will be denied. In order to increase the likelihood that this process will be completed successfully, you should contact the authorizer and indicate the following:

- You have applied to be the PACS Supervisory User for your filing institution.
- You have identified this individual as the authorizer of your identity and designation as a PACS Supervisory User.
- A third party organization will be calling to ask questions in this regard.
- He/she should respond positively to the third party organization's questions, verifying your role as the Supervisory User as well as verifying the role of the backup Supervisory User, if applicable.

If the authorizer is aware of and prepared to verify this information, the third party organization will indicate to the ACES program vendor that you, and the backup Supervisory User if applicable, are approved to receive Supervisory User digital certificates.



4. Downloading the Digital Certificate

If your digital certificate application is processed successfully, you will receive an e-mail at the e-mail address you provided in your application indicating that you have been approved by the ACES program vendor and providing unique enrollment codes (labeled as Pre-Authorized Numbers in the notification e-mail) for both yourself and your back-up Supervisory User, if applicable.

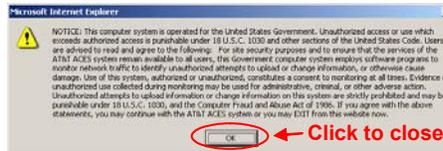
What happens if your digital certificate application is **NOT** approved?

If your digital certificate application was not approved, you will receive a rejection notification – also via e-mail. You will receive a rejection notification if the third party organization cannot contact or verify the authorizer you entered or the authorizer does not confirm you as the appropriate Supervisory User based on the information submitted. You should first contact your authorizer to determine if he/she was contacted by the third party organization and responded positively. If this is the case, you should contact the third party vetting organization to determine the reason you were not approved. If the authorizer was never contacted, you should double check the information you submitted on your application and re-apply with the corrected information.

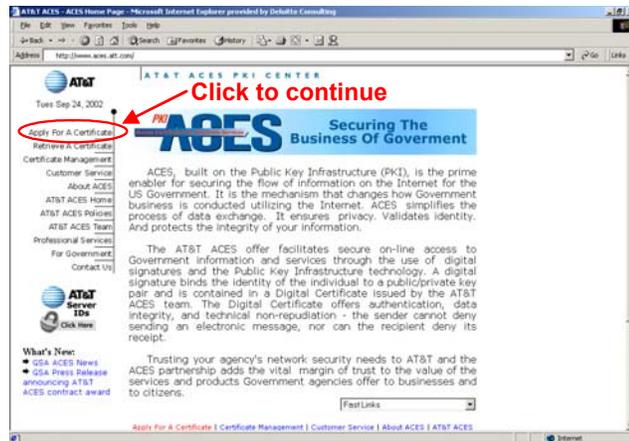
Once you have received your approval notification, with unique enrollment codes included, you should proceed by retrieving your digital certificate. (*Note: Set the back-up Supervisory User's enrollment code aside and do not distribute it – instructions regarding when this code should be distributed will follow later in this document.*) The digital certificate retrieval process supports both Netscape and Microsoft browsers; however, the process may vary slightly depending upon the browser and browser version you are using. Instructions are included for the most common versions of both Internet Explorer (version 5.x) and Netscape (version 4.x), but please be aware that certain steps may differ slightly depending upon your browser. The process for retrieving your digital certificate is as follows:

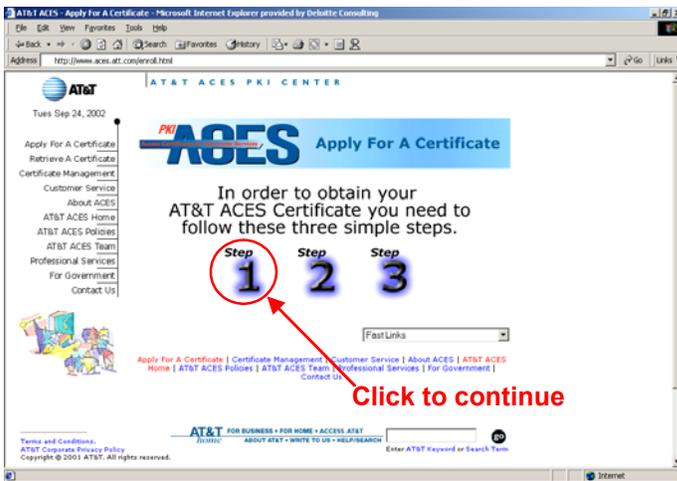
Note: You must complete all of the certificate retrieval steps on the same computer using the same Internet browser in order to successfully install the certificate.

1. Access the ACES program vendor's enrollment website at <http://www.aces.att.com>.
2. A *Government Notice* will appear on top of the ACES program vendor web page. After reading this notice, click the **OK** button.



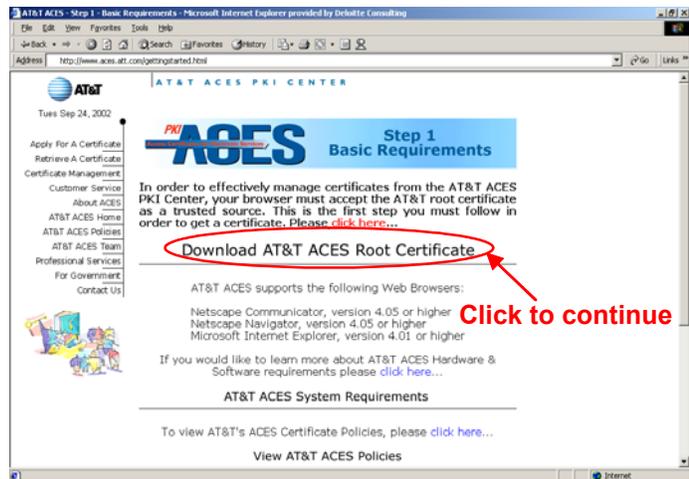
3. Once the Government Notice disappears you will see the AT&T ACES program homepage. Click the **Apply For A Certificate** link.





4. On the *Apply For A Certificate* webpage that appears, select the **Step 1** graphic.

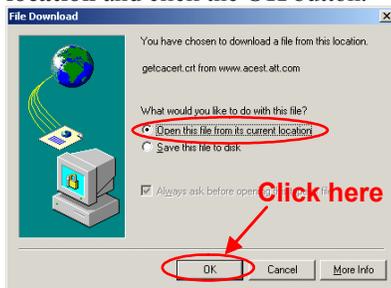
5. On the subsequent page, click the **Download AT&T ACES Root Certificate** link. You may want to review the hardware and software requirements to be sure that you are in compliance.



6. If a pop-up window appears, simply click **OK** to continue.

Internet Explorer Users Continue Here

7. On the *File Download* window that appears, select **Open this file from its current location** and click the **OK** button.



Netscape Users Continue Here – Note: If you are using Netscape 6.x the next 4 steps may be completed in a single step.

7. You will navigate through a series of *New Certificate Authority* windows. Click **Next** on the first three, accepting any default values.





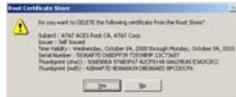
- Now a *Certificate* window will appear. Click the **Install Certificate** button.



- Next a series of *Certificate Manager Import Wizard* windows will appear. Click the **Next** button, click the **Next** button again, and then click the **Finish** button as you navigate through these three windows.



- The *Root Certificate Store* window should now appear and you will be asked to confirm that you want to add the digital certificate to the root store. Click the **Yes** button.



- Another *Certificate Manager Import Wizard* window will appear indicating that the install was successful. Click the **OK** button.



- You will now be returned to the *Certificate* window. Click the **OK** button to close it.

- Finally, close the *Instructions* window by clicking the **I Have Finished – Close This Window** button.

- On the fourth *New Certificate Authority* window, check all three checkboxes in the upper left portion of the window and click the **Next** button.



- On the fifth *New Certificate Authority* window, click the **Next** button, leaving the checkbox empty.



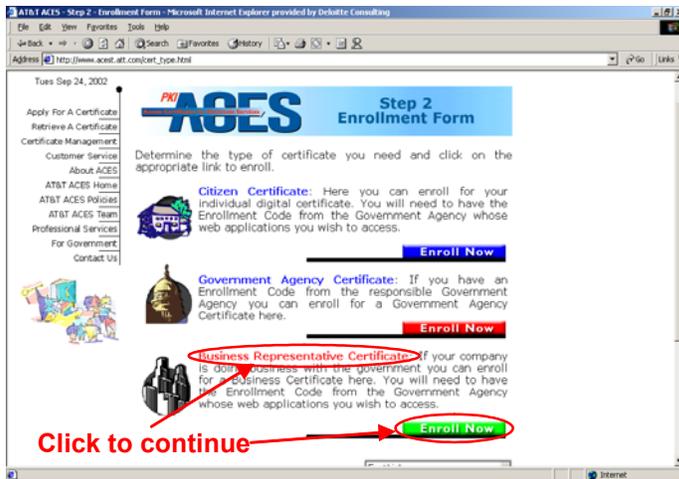
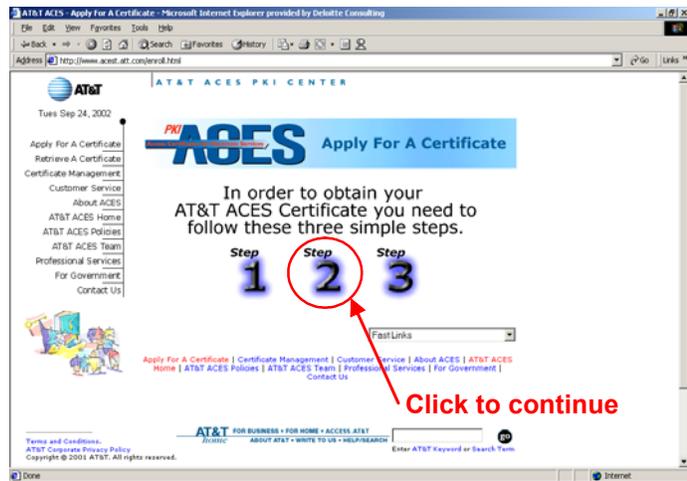
- In the final *New Certificate Authority* window, enter **AT&T ACES Root CA** in the **Name:** textbox and then click the **Finish** button.



- Skip to step 13.

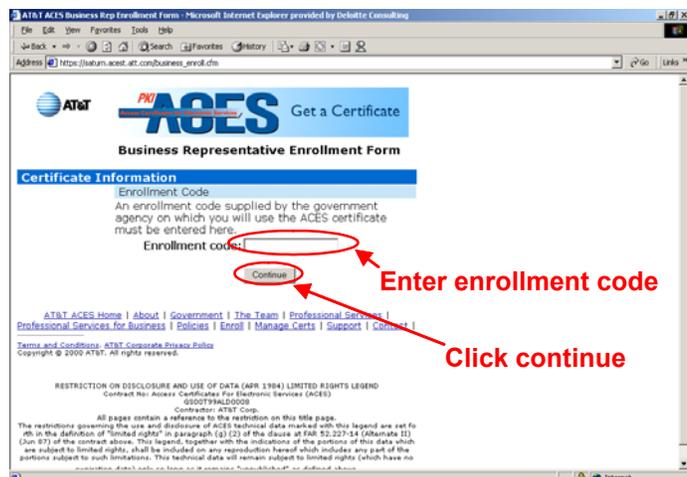


14. You should now be returned to the *AT&T ACES Apply For A Certificate* webpage. (If not, enter the URL <http://www.aces.att.com/enroll.html> into your browser.) Click the **Step 2** graphic to proceed with the next step.



15. The next page will require you to select a certificate type. Select the **Business Representative Certificate** link or the green **Enroll Now** button beneath it.

16. You should now be prompted to enter an enrollment code. If you receive a *Security Information* window first, click the **Continue** button to proceed. Enter the enrollment code exactly as it was provided by the ACES program vendor in their approval notification e-mail (labeled 'Pre-Authorized Number') and click the **Continue** button. *Note: Codes are case sensitive and must include the dash ('-') after the first character.*



Note: If you receive a message indicating that your enrollment code has already been used, contact the PACS Help Desk immediately at 1-888-827-2778 and select option 6.



17. If you successfully enter a valid enrollment code, you will be prompted to complete the *Business Representative Enrollment Form*. Enter information as requested on the webpage, keeping in mind that fields with bold labels are required. Enter a phrase of your choice in the **Shared Secret** textbox; you will only need this shared secret if you later wish to revoke or replace your digital certificate. When you have finished entering information, click the **Continue** button at the bottom of the page.

18. All of the information entered will now be presented back to you in a confirmation page. Please verify that all the information is correct. If not, click the **No** button at the bottom of the page to return to the previous page and correct the erroneous information. Otherwise click the **Yes** button to continue.
19. Next you will be presented with the **Business Rep AT&T ACES Subscriber & Usage Agreement**. Read this agreement. At the bottom of the page, prior to accepting or declining the agreement, you must select a *Cryptographic Service Provider* or *Encryption Strength*, depending upon your browser type.

Internet Explorer users must select **Microsoft Base Cryptographic Provider v1.0**

Netscape users must select **1024 (High Grade)**

After you have made the appropriate selection, click the **Agree** button. If you click the **Decline** button, the enrollment process will end and you will not be able to obtain a digital certificate from the ACES Program Vendor and subsequently will not be able to access PACS. If you receive a warning message, click **Yes** to continue.



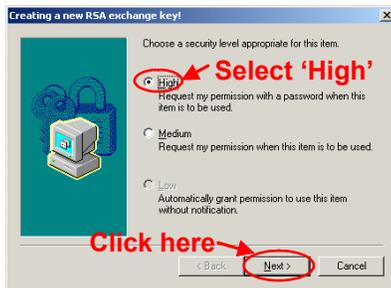
Internet Explorer Users Continue Here

Note: The following steps are extremely important and directly affect the security of your digital certificate. Please devote special attention to completing these steps accurately.

- 20. A window will appear titled *Creating a new RSA exchange key!*. Click on the **Set Security Level...** button.



- 21. On the next window, select the **High** radio button and click the **Next** button.



- 22. In the third window, you will see three empty textboxes. In the first textbox, labeled *Password for:*, enter a descriptive name for your digital certificate (e.g., John Doe PACS Certificate). In the second and third textboxes, labeled *Password:* and *Confirm:*, enter and then re-enter a password of your choice to protect your digital certificate. When done, click the **Finish** button.



Note: It is very important that you remember or record the password you entered in this step. This password will be required every time you attempt to use your digital certificate.

Netscape Users Continue Here

- 20. In the *Generate a Private Key* window, click the **OK** button to generate a new public/private key pair.



- 21. If you already have a Communicator Password, Netscape will prompt you to enter it. Enter your password and click the **OK** button.



- 22. If you do not have a Communicator Password you will be presented with the *Setting Up Your Communicator Password* window. Enter a password of your choice in the **Password:** textbox and then re-enter it in the **Type it again to confirm:** textbox. When finished, click the **OK** button.





23. On the final *Creating a new RSA exchange key!* window, verify that it reads “**Security level set to High.**” If not, repeat the previous three steps. Click the OK button.



Note: While Netscape does not require you to set up a Communicator Password, it is critical that you do so. The existence of a Communicator Password directly affects the security of your digital certificate.

Note: It is very important that you remember or record your Communicator Password. This password will be required every time you attempt to use your digital certificate.

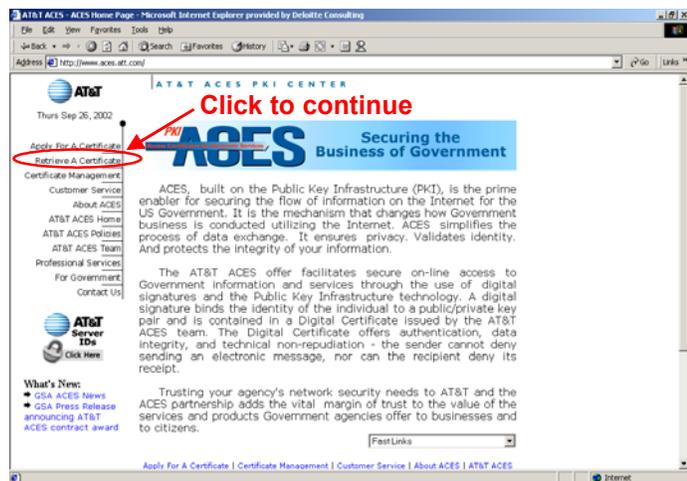
24. You may be prompted to create a private key container for Microsoft Windows. If not, move on to Step 25. If so, follow the instructions in the *Private Key Container* windows that appear.

23. Skip to Step 25.

25. Once you have completed these browser-specific steps you will see the *Business Representative Enrollment Submitted* web page. This page contains all of the information you entered in the previous steps. **Print this page and retain it for your records.** We recommend writing the password you entered for your digital certificate on this page so that all your information is retained in one place. However, be extremely careful not to share this password with others.

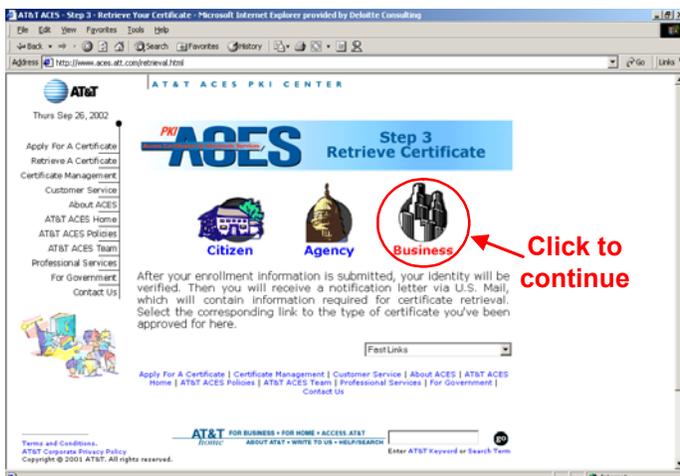
Note: Within one business day you should receive an e-mail from the ACES program vendor at the e-mail address entered in Step 17 containing a PIN which will allow you to complete the remaining certificate download steps. We recommend you bookmark this page and return when you have received this e-mail.

26. Once you receive the PIN notification e-mail, return to the ACES program vendor’s web page at <http://www.aces.att.com>, click **OK** if you receive a Government Notice pop-up window, and select the **Retrieve A Certificate** link.

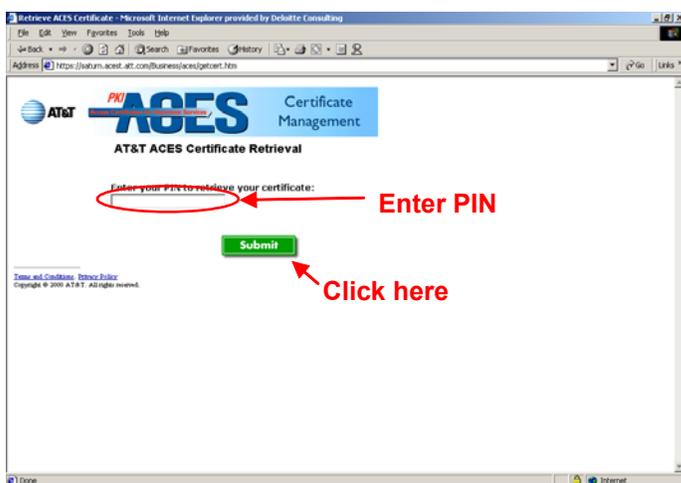




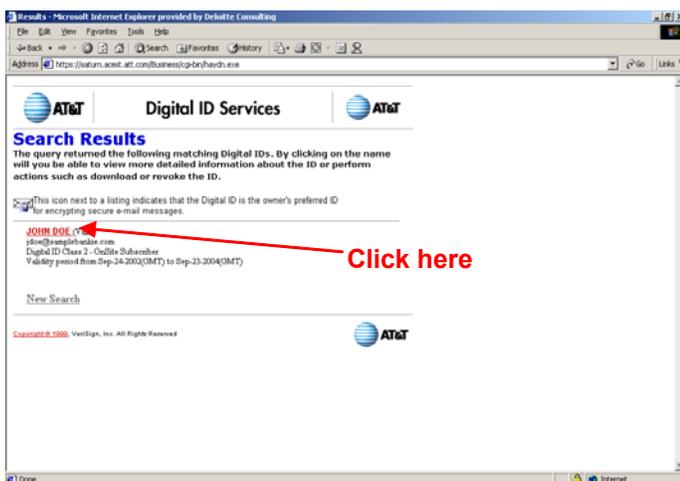
27. On the next screen, click on the graphic labeled **Business**.

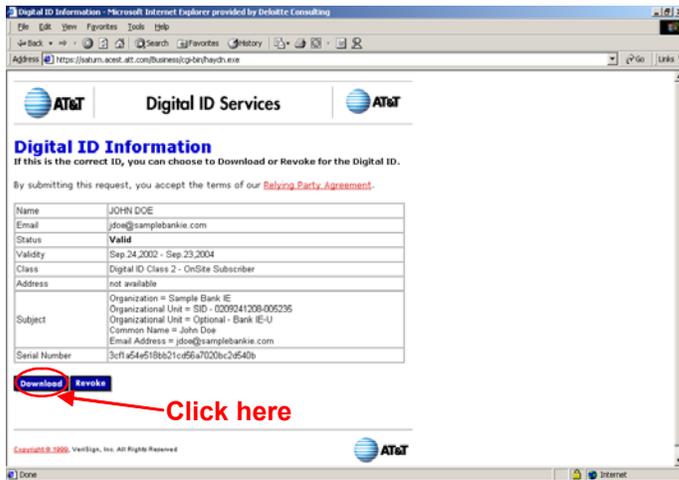


28. You will now be prompted to enter a PIN to retrieve your digital certificate. Enter the PIN provided in the e-mail you received from the ACES program vendor after completing step 25. Click the **Submit** button.



29. The next page will be titled *Digital ID Services*. On this page you should see your name, as a hyperlink, along with additional certificate information. Click on the link that is your name.





30. The next *Digital ID Services* web page will provide you with detailed information about your digital certificate along with options to download or revoke the certificate. Click the **Download** button.

31. The next *Digital ID Services* web page will prompt you to select a format to download the digital ID. The **ID Format** selection depends upon your browser. The correct selections are shown below. After selecting the appropriate ID Format, click the **Submit** button.



Internet Explorer users must select **My ID for Microsoft Internet Explorer/Outlook Express/Outlook**

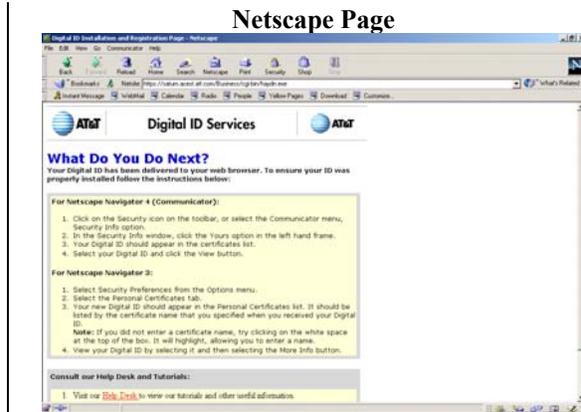
ID Format:

Netscape users must select **My ID for Netscape Navigator/Communicator**

ID Format:



32. The final *Digital ID Services* web page should provide an indication that you have successfully retrieved your digital certificate. If you are prompted with a warning message, click **Yes** to continue.



If you receive a page that looks different from the examples shown above, contact the PACS Help Desk at 1-888-827-2778 (option #6) or PACSHelp@notes.tcs.treas.gov for assistance downloading the certificate.

Responsibility of digital certificate possession

ACES digital certificate users are subject to subscriber obligations stipulated at the time of the digital certificate application process. Please contact the certificate issuer for questions regarding these obligations (ACES Certificate Policy can be found at <http://www.aces.att.com/policydocs/cp.doc>). FinCEN requires PACS users to abide strictly by these obligations.

Note: If you are using a Netscape browser, see Appendix A, Netscape Security Settings, for instructions on optimizing the interaction of your new digital certificate with your Netscape browser. It is recommended that you update your browser settings before proceeding with the next enrollment step.

You have completed the process of downloading your digital certificate. **Please restart your Internet browser and then proceed with Section 5 of this guide, *Enrolling in PACS*.**

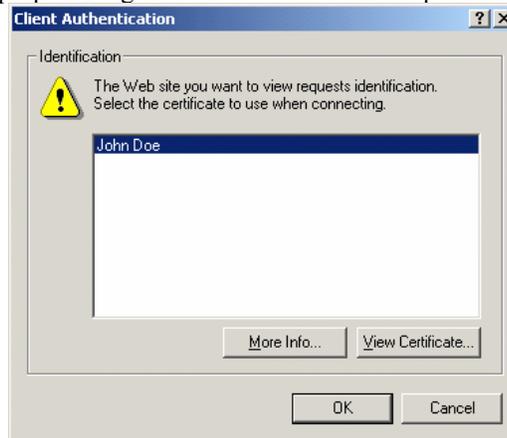


5. Enrolling in PACS

Enrolling in PACS requires that you have previously obtained your digital certificate, as discussed in the previous section, *4. Downloading the Digital Certificate*. If you have previously obtained your digital certificate, follow the steps below to enroll in PACS:

Note: If you have just completed Section 4 of this guide (Downloading the Digital Certificate), please restart your Internet browser before completing the steps in this section.

1. Access the PACS public website at <http://pacs.treas.gov/> and select the **Log Into PACS** link from the left navigation menu.
2. You will be presented with a government warning. Select the **Continue** button.
3. Before reaching the PACS secure site you will be prompted for your digital certificate. If your digital certificate is not selected automatically (only occurs if you alter your digital certificate security settings), select the appropriate digital certificate from the list provided and then select **OK**.



4. After selecting your digital certificate, you will be prompted to enter the password that protects the certificate. Enter your digital certificate password and click the **OK** button. **Note: Depending upon your system configuration you may be prompted to enter your password several times. If you do not enter the correct password you will receive an error indicating, "Page Cannot Be Displayed."** If this occurs, use the **Back** button on your browser to return to the PACS homepage and start over again by selecting the **Log Into PACS** link.





5. If you enter the correct password, PACS will recognize that this is the first time you have entered the secure site and will also recognize that you are a Supervisory User. PACS will first prompt you to enter your contact information. Contact information includes the following:
 - **First Name** (First) – First Name is a required field that is pre-populated based on information contained in your digital certificate.
 - **Last Name** (Last) – Last Name is a required field that is pre-populated based on information contained in your digital certificate.
 - **Telephone Number** (Tel) – Telephone Number is a required field that you must enter.
 - **E-mail Address** (Email) – E-mail Address is a required field that is pre-populated based on information contained in your digital certificate.
 - **User ID** – Your User ID is automatically assigned by PACS. You cannot edit this field.
 - **Filing Institution Enrollment Code** – *As the first Supervisory User for your filing institution you should leave this field empty. This code will be generated by PACS and provided to you later in the enrollment process. Subsequent users will then be required to enter this code when they enroll.*

FinCEN filer Registration:

Contact Info:

First: John Last: Doe

Tel: (555) 555-9999 Email: jdoe@samplebank.us

User ID: 81009376992

Financial Institution Enrollment Code:

Submit

After you have entered and verified your contact information, click the **Submit** button to continue.

6. Next you will be prompted to enter information about your filing institution. Filing institution information includes:

- **Institution Name** – required
- **Address** – required
- **City** – required
- **State** – required
- **Zip Code** – required
- **EIN** (Employer Identification Number) – required
- **MICR Number** (Magnetic Ink Character Recognition Number) – not required
- **TCC** (Transmitter Control Code) – the TCC is only required if your institution currently files CTR or SAR batches
- **Federal Regulator or Examiner** – required

FinCEN Institutions Registration:

Institution Info:

Institution Enrollment Code:

Institution Name: First Bank Address: 721 Main Street

City: General State: NY

Zipcode: 12345 EIN: 123456789

MICR #: 123456789 TCC:

Federal Regulator or Examiner: Federal Deposit Insurance Corporation (FDIC)

Submit

After you have correctly entered your filing institution information, click the **Submit** button.

7. You will now be presented with the PACS secure site homepage. At this time, PACS will also e-mail your institution's filing institution enrollment code to the e-mail address captured during enrollment.



Congratulations, you have successfully enrolled in PACS but before you attempt to begin using PACS you should do the following:

- **Download the PACS User Manual and Supervisory User Manual** – On the PACS secure site homepage you will see a left navigation menu listing all of your regular user and Supervisory User privileges. Also on the left navigation bar you will find links to the User Manual and Supervisory User Manual.
 - The User Manual is a comprehensive guide to all the standard PACS functionality including user enrollment, CTR & SAR filing, receiving Alerts, and Secure Messaging communication with FinCEN.
 - The Supervisory User Manual is a comprehensive guide to all the PACS functionality that is specific to Supervisory Users, including initiating user enrollment, managing user access, maintain filing institution information, and tracking the status of all filings from the institution.
 - **Create a back-up copy of your digital certificate** – Your digital certificate along with the password that protects it is the only thing that can authenticate you to PACS. In order to prevent losing access to PACS in the event that your computer crashes or you upgrade to a new system you must back-up your digital certificate. To back-up your digital certificate, follow the instructions that are specific to your Internet browser for ‘*Exporting a Digital Certificate*’ in Section 3.3 of the PACS User Manual.
 - **Provide enrollment materials to the back-up Supervisory User** – Now that you are successfully enrolled in PACS you should provide the necessary materials to your back-up Supervisory User, if applicable, for him/her to enroll successfully. Your back-up Supervisory User will need the following information:
 - *ACES Program Vendor’s Enrollment Code* – Based on the information contained in the e-mail you received from the ACES program vendor, you must provide the back-up Supervisory User with his/her enrollment code (labeled ‘Pre-Authorized Number’ in the notification e-mail). He/she will use this enrollment code to complete the certificate application on the ACES program vendor’s website.
 - *Filing Institution Enrollment Code* – You must provide the back-up Supervisory User with your institution’s filing institution enrollment code. This code should have been e-mailed to you after completing enrollment. It is also available by selecting the **View FI Enrollment Code** link on the left navigation menu of the PACS secure website.
- Note: It is extremely important that the back-up Supervisory User have the appropriate filing institution enrollment code when they enroll in PACS. The filing institution enrollment code is what associates them with your filing institution. If it is incorrect, they will be unable to participate in PACS as a member of your filing institution.***
- *Enrollment Instructions* – You should download and provide the PACS User Manual to the back-up Supervisory User. Instruct the back-up Supervisory User to refer to Section 3 of the PACS User Manual for instructions on obtaining a digital certificate and Section 4 for instructions on enrolling in PACS.
- **Initiate the enrollment of additional PACS users** – If there are additional individuals in your institution that will need access to PACS you should initiate the enrollment of these individuals at this time. The introductory portion of Section 3 of the User Manual will help you determine who within your institution needs a digital certificate. Section 3 of the Supervisory User Manual (*Initiating the Enrollment of Your Institution’s Users*) contains detailed instructions for completing this task once you have determined who needs a certificate.

Note: Now that you have successfully completed enrollment as the initial Supervisory User you may discard this guide. The User Manual and Supervisory User Manual contain all the information you will need from this point forward.



Appendix A: Netscape Security Settings

To maintain the highest level of security when interacting with PACS, your digital certificate should be password protected. In addition, you will want to minimize the number of times you are prompted to enter your password during a PACS session. If you are using Internet Explorer these items are set appropriately during the certificate download and installation processes. If you are using a Netscape browser (4.x or 6.1 and up), you will need to perform additional steps to configure your browser security settings.

Security Settings for Netscape 4.x

1. Open your Netscape browser.
2. Open the *Security* window by selecting **Communicator – Tools – Security Info** from the menu bar (or press Ctrl+Shift+I).
3. Select the **Passwords** link on the left navigation bar to open the passwords window.
4. Select the radio button next to the **The first time your certificate is needed** option under the *Communicator will ask for this Password* heading.
5. Select the **Navigator** link on the left navigation bar to open the navigator window.
6. In the drop down box under the heading *Certificate to identify you to a web site*: select **Ask Every Time**.
 - a. If you have only one digital certificate listed you can select this one instead of selecting **Ask Every Time**. However, if you add another digital certificate in the future you must remember to go back and change this setting.
7. Click on the **OK** button to save the settings and close the *Navigator* window.

Security Settings for Netscape 6.1 and Above

1. Open your Netscape browser.
2. Open the *Preferences* window by selecting **Edit – Preferences...** from the menu bar.
3. Click on the arrow next to **Privacy & Security** on the left navigation bar then click on the **Master Passwords** link.
4. In the *Master Password Timeout* portion of the *Master Passwords* window select the radio button next to **The first time it is needed**.
5. Click on the **Certificates** link on the left navigation bar.
6. In the *Client Certificate Selection* portion of the *Certificates* window select the radio button next to **Ask Every Time**.
7. Click on the **OK** button to save the settings and close the *Preferences* window.

If these settings have been made properly, you will now be prompted to enter your digital certificate password any time you enter PACS and then only when you are signing electronic BSA filing forms. To change this password, you should follow steps 1 through 3 above then click on the **Change Password** (or **Set Password** for Netscape 6.1 and above) button and follow the on-screen instructions.