Creating a Digital Certificate and importing to keychain for Adobe Acrobat Digital Signature Signing

- Basic Instructions
- Trusting the UT Austin Intermediate Certificate To Allow For Successful Validation of UT Employee Signed Documents

Adding a digital certificate to sign an Adobe PDF

Basic Instructions

If you don't already have a digital certificate:
go to https://certificates.security.utexas.edu/

Choose UT austin from the list and click select to get started and use your @austin.utexas.edu address

go to https://stache.utexas.edu/   and download your mail encryption key (download P12). It will be named encryption and mail signing cert. Use your EID and EID password to log in. You will also need to do the second factor Duo authentication.

The page with your encryption key has a password. you will need that password to import it into your keychain.

Double click the downloaded key file named something like YourEmailAddress.P12

for MAC:

It should automatically try to import into your keychain and will ask for the password for that file which was the password on the page where you downloaded the encryption key in the box that says "Encrypted File Password". enter that password. It may also need your EID password just to allow the importation into the keychain when it asks for your "login" password.

if you imported it successfully, there will be a Keychain list on the left, and also a Category list. click My Certificates in the Category pane and locate your certificate. Click the triangle beside your certificate so it shows your private key beside your email address. Double Click the Key icon with your email address.

if you get this far, click the Access Control tab. in the box underneath where it says "Always allow access by these applications:" click the + sign underneath and navigate your way to your Applications folder and add Adobe Acrobat Pro.app, or whichever version of Adobe Acrobat you're using. I usually add Mail.app so I don't have to go back at a later date to set them up for email signing and encryption. Don't bother with Mail.app if you use Outlook for email.

Save Changes. it should ask for your "login" (EID password) password again.

FOR Windows:

Double clicking the p12 file will open Certificate Import Wizard.
Go through. You shouldn't have to tick off anything. Do not check the box to force strong protection or it will make you enter your password every time you want to use the key.

Finish the wizard.

in Acrobat:

Then open Acrobat Pro/Acrobat Reader and go to the Acrobat menu (Edit menu on Windows) and choose Preferences. scroll down to Signatures.

on the right is Identities & Trusted Certificates. Click More.

under Digital IDs, your name should show in the right panel. click on it and under Usage Options do for each item one time: Use for Signing. Use for Encryption. Use for Certifying.

click Trusted Certificates.

1. click the blue Import button up top of that window.
2. in the left pane, you'll also want to click Trusted Certificates and find the The University of Texas at Austin RSA CA certificate and Import it. To import it, you click browse and go find it in your downloads folder if you downloaded it via this wiki, or if one of us helped you, we might have just dragged it to your desktop.
   once you do that. it should now be imported.
3. click on the certificate you just browsed for and opened and it should show in the Contacts box. it should show down below in the lower Certificates pane. You'll want to click on it and click the Trust button and let that certificate trust on every box that shows up.

- At this step for Acrobat Pro XI running on Windows 7 the following had to be done to add the University's signing certificate to the list of trusted certificates. If you don't do this step then Acrobat reader will always says UT signing certificates are invalid because the certifying certificate is not trusted.
    - In the same window where you did the previous step, double-click on the user's listed certificate in the right pane
    - In the window that appears you will see a tree of signing certificates in the left pane. Just above the botton branch where the user's certificate is listed, a parent certificate named "The University of Texas at Austin" is listed. Click that certificate to bring up its options in the right pane.
    - Click the "Trust" tab and then click the button labeled "Add to Trusted Certificates..."
    - Accept the default trust options of just trusting it for signing and certifying documents
    - Click OK to accept all changes

*If you do not see a certificate for The University of Texas at Austin RCA, find it in the Certificates section of the Keychain app and drag it to the desktop, then you can import it into Adobe Acrobat.

This wiki page has an attachment for how to place a signature in Acrobat

Trusting the UT Austin Intermediate Certificate To Allow For Successful Validation of UT Employee Signed Documents

When someone uses their UT assigned digital certificate to sign a document by default new installations of Adobe Acrobat/Reader will not trust the signature which will result in a warning being displayed when people open up the signed document and verify the authenticity of the certificate used to sign the document. This happens because the certificate company that UT uses for their certificates is not currently built into and trusted by Adobe Acrobat /Reader. So you have to manually trust at least one of the parent certificates in the certificate chain used to generate UT employee digital certificates. This manual trust has to be done on a per-user account basis so if you have multiple users on a computer, each user account will need to go through the process of trusting the parent certificate. You can either manually open up the Adobe Trust Manager in Adobe Acrobat/Reader, select the parent certificate, and then select the option to "trust" it OR do the following:

1. Ensure Adobe Acrobat/Reader is installed on the target computer.
2. Download this exported certificate file. This is the UT Austin intermediate certificate used to generate all UT Austin employee digital certificates.
3. You can go back to your downloads and ctrl click on the CertExchangeUTRSA.fdf file, or right click on it, and tell it to open with Adobe Acrobat pro. It may present you with a window that says Set Contract Trust which you can click to get to step 4 depending on the version.
4. You will be presented with a Window to trust the certificate. Check off all options as shown in the following screenshot:
    a.
5. Done. Restart Adobe Acrobat/Reader to put the change into effect. Now when you verify the UT employee digital certificate used to sign a document it should show up as valid.

Adding a digital certificate to sign an Adobe PDF