Introduction

Congratulations on purchasing your Ensured PDF signature, which allows you to easily provide PDF documents with a trusted digital signature.

The token is provided by us with the temporary password that was entered during the order, it is important that you know this password before starting the next steps below. The token is a secure cryptographic device that locks itself after entering the password incorrectly several times.

Please remember to save your token password!

The token currently only contains the so-called private key, on which the certificate is based at the time of issue. Using the "Initialize" function will block the token for good, so please don't use this function!

The token will soon be the carrier of the certificate, so if multiple people use the same token, only one installation will be needed, and the configured password will have to be shared. It is necessary to install the driver software of the token on every workstation on which the token will be used.

By following the steps below you will soon be able to provide the first PDF with an Ensured digital signature:

1. Driver software installation
2. Change temporary password
3. Download certificate files
4. Installation certificate files on token
5. Configuration Adobe Acrobat
6. Place your first digital signature

1. Driver software installation

To use the Ensured PDF signature, it will have to be installed on the supplied token after it has been issued. For this you will first have to install the necessary driver software. You can download the drivers from the Ensured support page; https://www.ensured.nl/support

Depending on the type of token that is supplied, one of the following applies. Which model has been delivered is stated in the delivery letter.

- Feitian ePass2003 Client software
- Safenet Authentication Client software

If this type of token has aready been used in your organization, it is advisable to check the current software version and update to the latest version if necessary.

2. Change temporary password

As soon as the installation of the software is completed, you can start the software to change the temporary password to your own password. Please note that this password must be remembered, as the token will lock itself if you enter the password incorrectly several times. A password manager is recommended for this.

2a. Change password with SafeNet tokens

Follow the steps below to change the temporary password of a SafeNet token;

1. Launch the SafeNet Authentication Client Tools software.
2. Connect the token to the computer.
3. In the SafeNet Authentication Client Tools application, click the gear (settings) icon at the top
4. Right-click on the 1st item under "tokens", presumably "Ensure e-Sign USB" and select "Change Password ..."
5. Now enter the temporary password at "Current Token Password" and the desired new password in the two lower fields.
6. Click "OK" to set the new password.

2b. Change password with Feitian tokens - Windows

Follow the steps below to change the temporary password of a Feitian token;

1. Start the Feitian Manager application.

2. Connect the USB token to your Windows machine.
3. After a few seconds, press **Control + Alt + Delete**.
4. Select **Change Password** from the list of options shown.
5. Click **Login Options** just above the Cancel button.
6. Click the **Smartcard** icon next to the key icon.
7. You will now see the token type and fields for old and new pin code.
8. Enter the old (temporary) password in the first field.
9. Enter the new password in the 2nd field and repeat this password in field No. 3.
10. Click the right arrow in the third field to save the new password.

2c. Change password with Feitian tokens - MacOS

Follow the steps below to change the temporary password of a Feitian token;

1. Insert the token into one of your Mac's USB ports
2. Open the 'EnterSafeCastleAdminMgr.app' application from the Applications folder.
3. Click the **Change User PIN** button at the bottom of the window.
4. Enter the set, temporary password in field 1.
5. Enter the new password in fields 2 and 3.
6. Click **OK** to save the new password.

3. Download certificate files

The ordered certificate will only be issued when the sent verification code is sent via the Ensured collection form. For this purpose, a separate email message from ensured.com has been sent to the email address specified during the order. This message contains a unique URL, along with a verification code. As soon as the Verification Code has been entered and the "Get" button is pressed, the certificate will be created and after ten seconds the download will follow in the form of a "certificate.cer" file.

Together with your own certificate, the so-called CA certificates will also have to be installed on the token, you can download these separately via the URL below:

https://www.ensured.com/support/Ensured_Downloads/Ensured_Root_certificates

4. Installation certificate files on token

After downloading the new certificate, open the Feitian or Safenet management software, depending on the type of token you received with your order. Follow the steps at 4a for the SafeNet token, or 4b if you have received a Feitian token.

4a. Certificate installation on Safenet tokens

1. Open the Safenet Authentication Client Tools application.
2. Select the **advanced view** by clicking the gear icon.
3. Select your token on the left.
4. Click the import icon.
5. Enter the password to unlock the token.
6. Click the **Browse** button and select the .cer file downloaded from the Ensured collection form; your pdf certificate.
7. Click **import** again.
8. Click the **Browse** button and select the 'EnsuredRootCA.cer' file downloaded from the Ensured website.
9. Click **OK** to import the certificate.
10. Click **import** again.
11. Click the **Browse** button and select the 'EnsuredDocumentSigningCA.cer' file downloaded from the Ensured website.
12. Click **OK** to import the certificate.

4b. Certificate installation on Feitian tokens

1. Open the ePass Manager application.
2. Enter the password to unlock the token.
3. Click **import**.
4. Click the **Browse** button and select the .cer file downloaded from the Ensured collection form; your pdf certificate.
5. Select the * **Signature** * option at the bottom of this window and click **OK** to import the certificate. This step is important because otherwise the certificate will not be visible in Acrobat.
6. Click **import** again.
7. Click the **Browse** button and select the 'EnsuredRootCA.cer' file downloaded from the Ensured website.
8. Click **OK** to import the certificate.
9. Click **import** again.
10. Click the **Browse** button and select the 'EnsuredDocumentSigningCA.cer' file downloaded from the Ensured website.
11. Click **OK** to import the certificate.

Now your token is ready to be configured with your PDF application. Please note:

- The certificate and private key are installed on the token and cannot be exported.
- It is possible to use the token on multiple machines, but only one at a time.

When this step is completed, you can use your certificate!

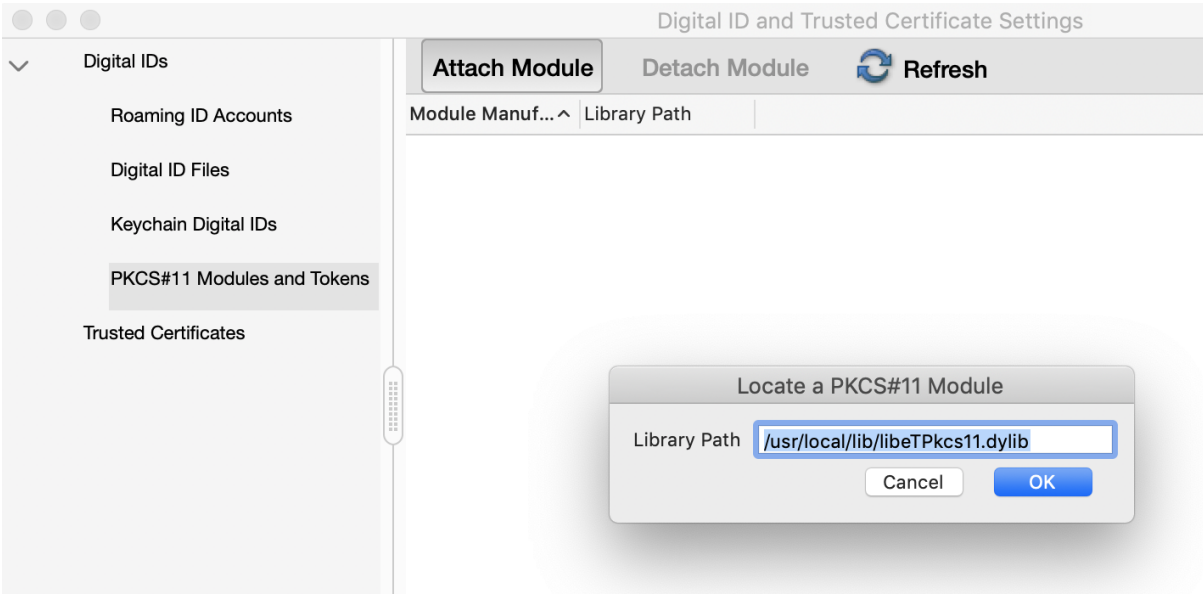
5. Adobe Acrobat configuration

The Ensured PDF signature is trusted by default in Adobe Reader by inclusion in the Adobe AATL list. In addition, you can also use Adobe for signing and / or time stamping PDF documents.

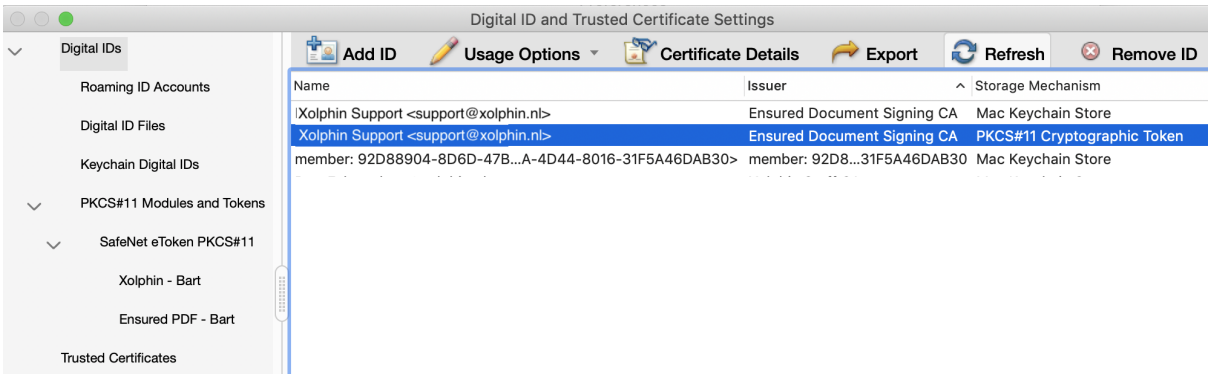
This guide applies to Adobe Acrobat Pro DC (version 2019.012.20034) and Adobe Acrobat Reader DC (version 2019.012.20034) and later versions. Prior to this configuration, the correct drivers must be installed as described in step 1 of this manual. Leave the token in the machine during the processes below.

Configuration of a PDF signing certificate in Adobe Acrobat

1. Start Adobe Acrobat.
2. Open the Preferences window (Windows: CTRL + K or Mac: ⌘ +,).
3. Select the **Signatures** category.
4. Click **More ...** under the **Identities & Trusted Certificates** category.
5. Click **Digital IDs** > **PKCS # 11** Modules and Tokens.
6. Click **Link Module**.
7. Enter the path to PKCS # 11 library, this is (if recommended drivers are installed).
8. For **Feitian** tokens;
    - On the Mac, the path is; **/usr/local/lib/libcastle.1.0.0.dylib**
    - For Windows, the path is; **C:\Windows\system32\eps2003csp11.dll**
9. For **Safenet** tokens;
    - On the Mac, the path is; **/usr/local/lib/libeTPkcs11.dylib**
    - For Windows, the path is; **C:\Windows\system32\eToken.dll**



10. After entering the path to the driver, click **'Ok'** to activate the token.
11. Click the appropriate token under PKCS # 11 Modules and Tokens on the right, click **Login**, enter the token password and click **Ok**.
12. Now click on **Digital IDs**.
13. Now select the certificate with the Storage mechanism: **PKCS #11 Cryptographic Token**.



14. Now click on **Usage Options** (pencil).
15. Now select **Use for signing** (or in Acrobat Pro **Use for Certifying**).
16. A pen or rosette will now appear in front of the name of the selected certificate.
17. Click **Close** and **OK** in the underlying dialog.

Adobe Acrobat is now configured to generate signatures with the certificate installed on the token.

5b. Configuring a Timestamp Server in Adobe Acrobat

By adding a timestamp to a PDF document in addition to a digital signature, your signature remains verifiable even if your PDF certificate is no longer valid.

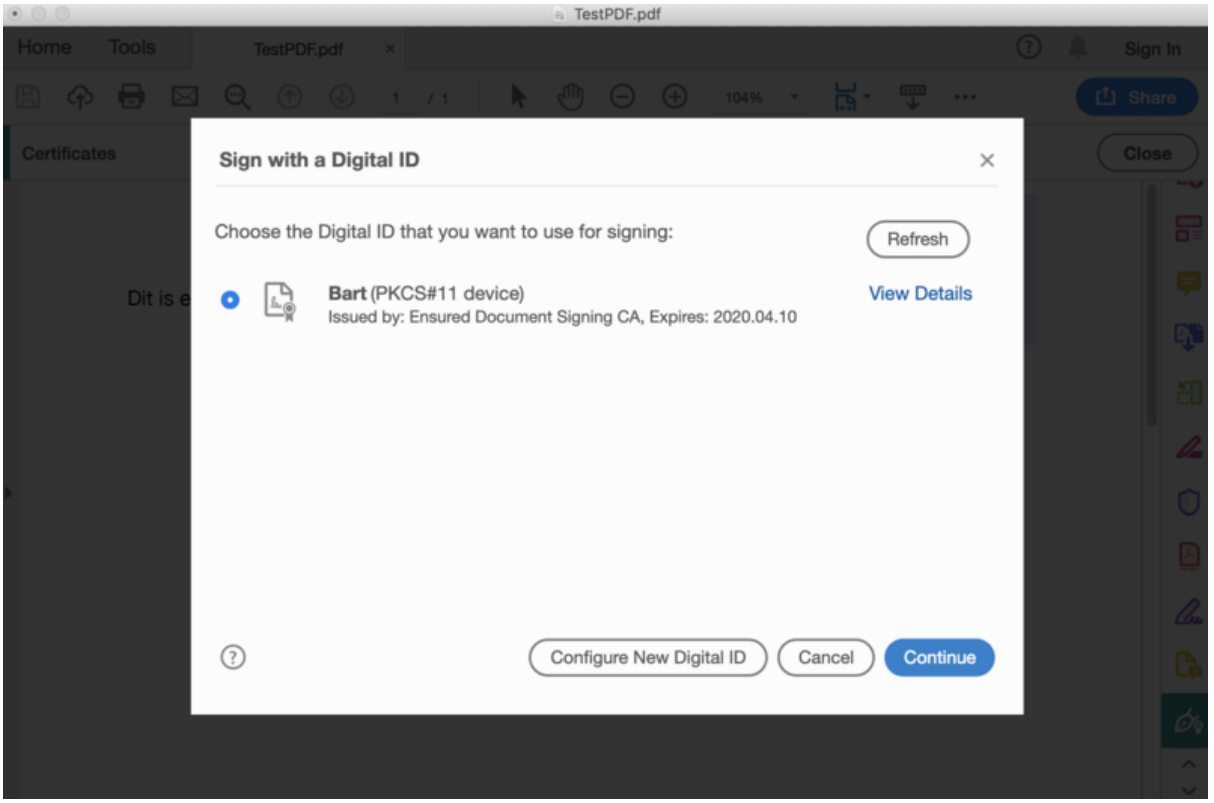
1. Start Adobe Acrobat.
2. Open the Preferences window (⌘ +,).
3. Select the **Signatures** category.
4. Click **More ...** under the **Document Timestamp** category.
5. Click **New**.
6. Enter a name (e.g. Timestamp server) and the server URL (for Ensured: http://timestamping.ensuredca.com)
7. Click **OK**.
8. Select the added Timestamp Server and click **Set Default.**
9. Click **Close** and **OK** in the underlying dialog.

Adobe Acrobat is now configured to also generate a timestamp during signature.

6. Placing your first digital signature

6a. Using a PDF signing certificate in Adobe Acrobat

1. Launch Adobe Acrobat and open a PDF document.
2. From the menu, click **Edit** and then **Manage Tools**.
3. Click **Certificates**.
4. An extra bar will now appear at the top, click here on **Digital signing** (or in Acrobat Pro on **Certify**).
5. Draw the requested **Signature box** anywhere in the document.
6. Select the certificate with the correct name and with the name (**PKCS # 11 device**) after the name and click **Continue**.



7. Now adjust the appearance of the signature if necessary, enter the token password and click **Sign**. Note: It is also possible to save multiple templates for signature appearances.
8. Save the PDF document.

The PDF document is now signed. If a Timestamp Server is configured as 'Default', this Timestamp Server will automatically be used to generate a timestamp for the PDF document. This timestamp is included in the signature.

6b. Using a Timestamp Server in Adobe Acrobat

Setting a seperate timestamp is only necessary when the Timestamp server is not set as default (see point 5b)

1. Launch Adobe Acrobat and open a PDF document.
2. From the menu, click **Edit** and then **Manage Tools**.
3. Click **Certificates**.
4. An extra bar will now appear at the top, click here on **Timestamp** (or if the Timestamp Server is set as 'Default', click on Digitally Sign).
5. Save the PDF document.

6c. Adding Multiple Signatures in Adobe Acrobat

It is possible to place multiple signatures on a PDF document. In order to place multiple signatures on a PDF, each signature field must be pre-placed before any signing takes place. While the signatures themselves can be placed with Adobe Reader or Adobe Acrobat, only the Standard & Professional version of Adobe Acrobat can pre-place these signature fields. The screenshots in this article are based on Adobe Acrobat Standard XI.

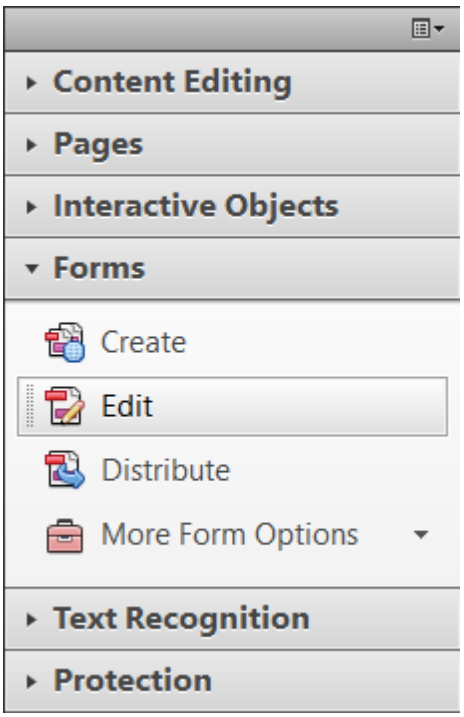
A workflow involving multiple signatures will use both the **Certify (Visible)** option and the **Sign With Certificate** option available in Adobe Reader & Adobe Acrobat. The initial signatures will all use the certify option, as this option allows additional signatures to be placed after signing. Only the final signature on the document will use the Sign With Certificate option, which will not allow for any modification or signatures once it is placed.

For example: if you have 5 signatures to place, the first 4 will be placed using the Certify (Visible) option and the 5th signature will be placed using the Sign with Certificate option.

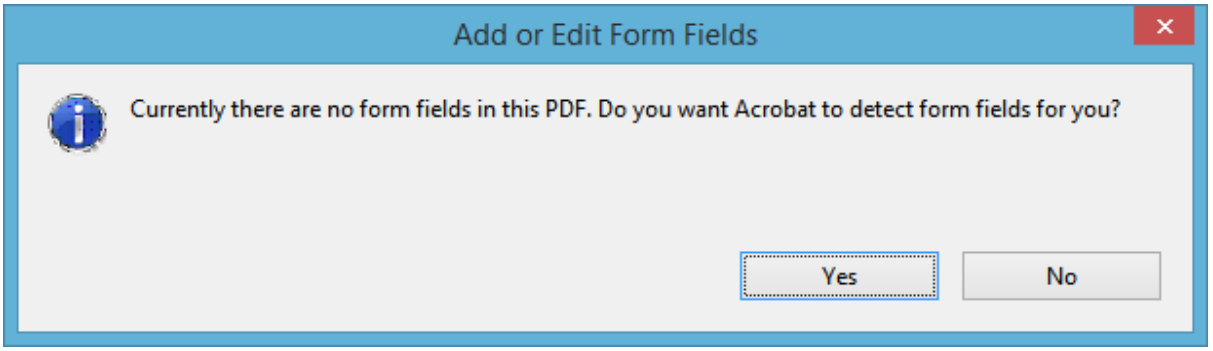
Adding signature fields

1. Open Adobe Acrobat
2. Click on the **Tools** menu on the upper right.

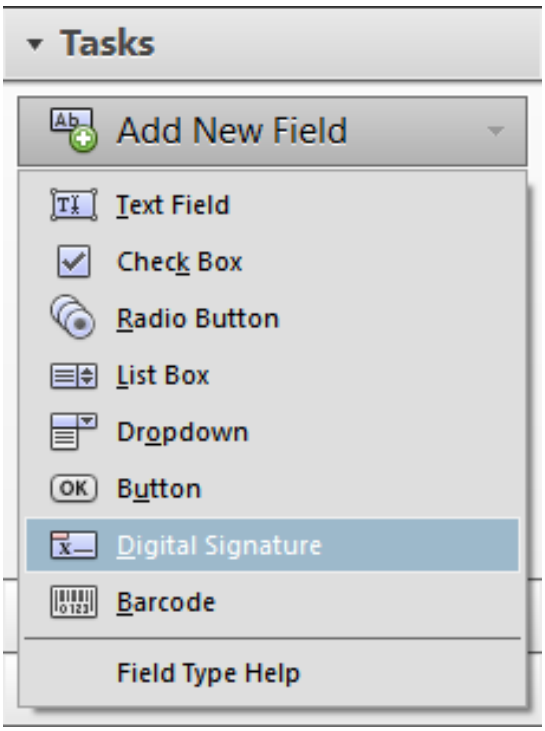
3. Expand the **Forms** section and click **Edit**.



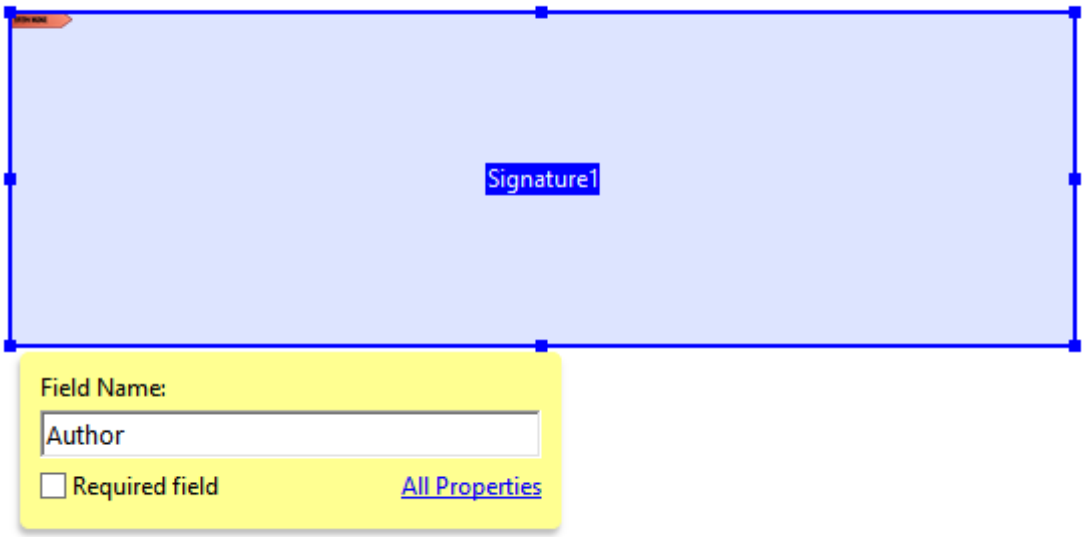
4. If prompted to auto-detect form fields, click **No**.



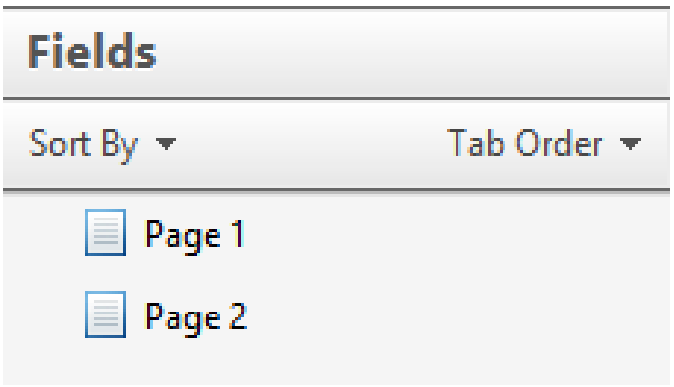
5. Under the **Tasks** section, click **Add New Field** > **Digital Signature**.



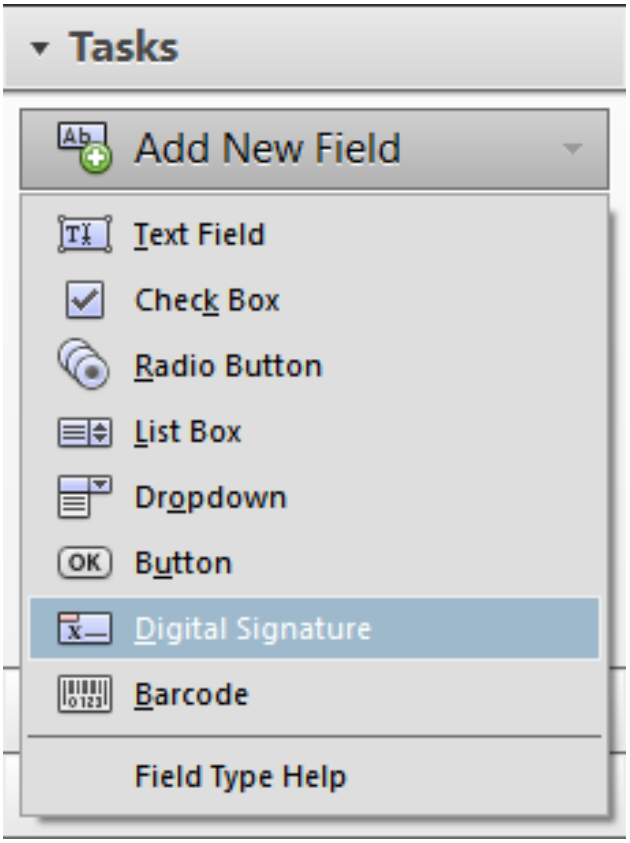
6. Drag a rectangle to create the desired size of the signature field. Optionally label the field for the intended signer (E.g. Author, Approver, QC, Witness, etc.)



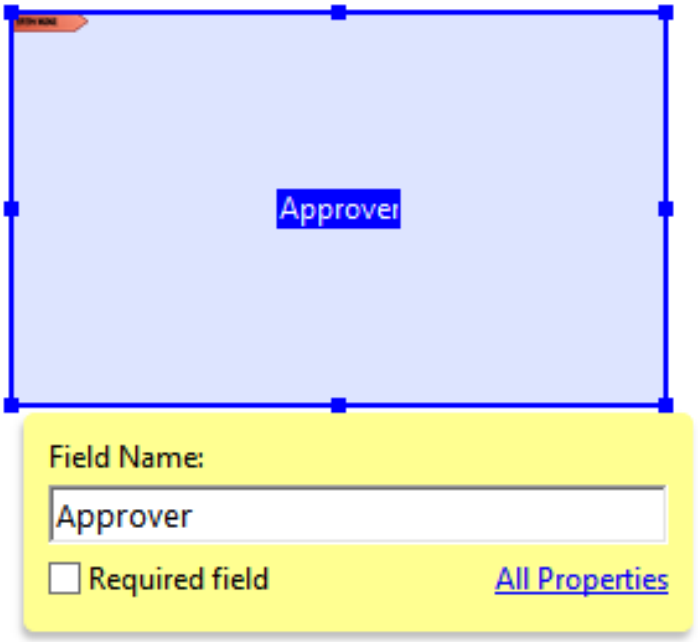
7. If your PDF has multiple pages and the next signature is on a different page, click the corresponding page under the **Fields** section to move to that page.



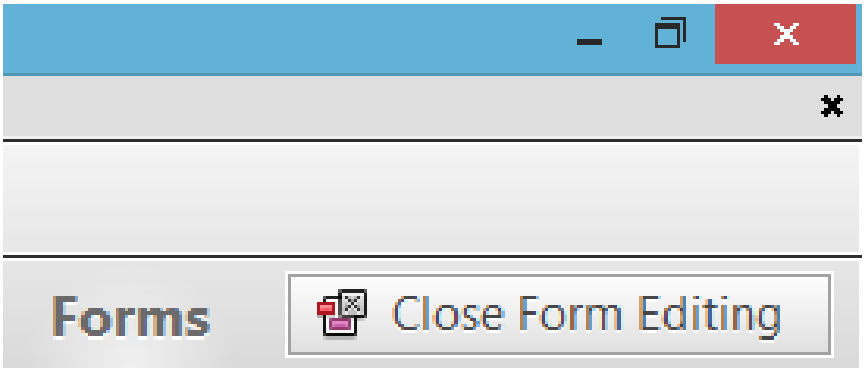
8. Again under the **Tasks** section, click **Add New Field** > **Digital Signature**.



9. Drag another rectangle to place the next signature field and optionally label it for the suggested signer.



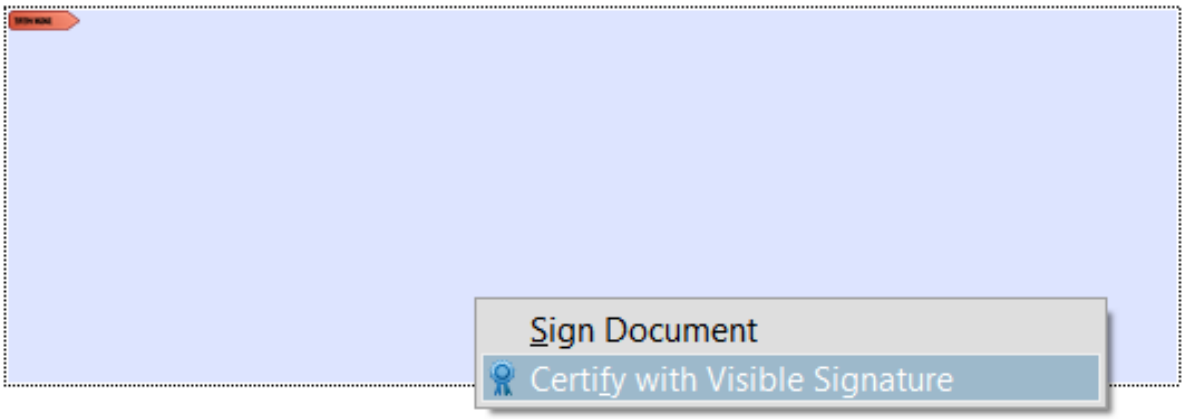
10. Repeat this process until all needed signature fields are in place.
11. When finished, click **Close Form Editing** to exit the form editor.



12. Save your PDF; the document is now ready for signing.

Placing Multiple Signatures

1. Open a PDF that contains multiple signature fields.
2. Right click the first signature field to be signed and choose the **Certify with Visible Signature** option.



The **Certify Document** window will appear.

3. If you have multiple certificates, choose your signing certificate from the **Sign As:** drop-down menu.
4. Customize the signature appearance to your liking.
5. Under **Permitted Actions After Certifying** make sure either **Form fill-in and digital signatures** or **Annotations, form fill-in, and digital signatures** is selected so that additional signatures can be placed.
6. Click **Sign.**
7. Save the PDF & enter the password for your Certificate/USB Token.

The next steps will vary depending on the number of signatures and whether or not one person is applying multiple signatures or multiple people are applying one signature each. If the next signature is to be placed by another individual, forward the certified document to them to complete the next signature field. If you are placing additional signatures with the same cert, right-click the next signature field and again choose **Certify with Visible Signature.**

If this is the final signature to be applied:

1. Click the signature field to bring up the **Sign Document** window.
2. Choose your certificate from the **Sign As:** drop-down.
3. Customize the signature appearance to your liking.
4. Check the box to **Lock Document After Signing**

   Note: an unlocked document cannot be altered, but filling form fields and adding signatures is allowed. After locking a document, none of this is possible anymore.
5. Click **Sign**.
6. Save the PDF & enter the password for your Certificate/USB token.

The document now has its final signature in place. All certifications and signatures should be valid and can be individually verified through the signature panel.