Inleiding

Gefeliciteerd met de aanschaf van je Ensured PDF handtekening, waarmee je gemakkelijk PDF documenten voorziet van een vertrouwde digitale handtekening.

Het token is door ons voorzien van het tijdelijke wachtwoord dat is opgegeven tijdens de bestelling, het is belangrijk dat je dit wachtwoord kent voordat je begint met de vervolgstappen hieronder. Het token is namelijk een beveiligd cryptografisch apparaat, dat zichzelf vergrendelt na het meermaals verkeerd invoeren van het wachtwoord.

Sla het token wachtwoord dus goed op!

Op het token staat momenteel alleen nog de zogenoemde private key, waarop het certificaat wordt gebaseerd op het moment van uitgifte. Het gebruiken van de 'Initialiseren' functie zal het token onbruikbaar maken, gebruik deze functie dus niet!

Het token is straks de drager van het certificaat, als meerdere personen gebruik maken van hetzelfde token zal er dus maar één installatie nodig zijn, en zal het geconfigureerde wachtwoord moeten worden gedeeld. Het is wel noodzakelijk om op ieder werkstation waarop het token gebruikt gaat worden, de driver software van het token te installeren.

Door het volgen van onderstaande stappen kun je straks de eerste PDF voorzien van een Ensured digitale handtekening:

1. Installatie driver software
2. Aanpassen tijdelijk wachtwoord
3. Downloaden certificaat bestanden
4. Installatie certificaat bestanden op token
5. Configuratie Adobe Acrobat
6. Plaatsen van je eerste digitale handtekening

1. Installatie driver software

Voor het gebruiken van de Ensured PDF handtekening zal deze na uitgifte op het hierbij geleverde token geïnstalleerd moeten worden. Hiervoor zul je eerst de benodigde driver software moeten installeren. De drivers kun je downloaden vanaf de Ensured support pagina; https://www.ensured.nl/support

Afhankelijk van het type token dat geleverd wordt is één van onderstaande van toepassing. Welk model er is geleverd staat op de bijsluiter.

- Feitian ePass2003 Client software
- Safenet Authentication Client software

Als er al langer met dit type tokens wordt gewerkt is het aan te raden de actuele softwareversie te controleren en eventueel bij te werken naar de nieuwste versie.

2. Aanpassen tijdelijk wachtwoord

Zodra de installatie van de software is voltooid kan deze worden opgestart om het tijdelijke wachtwoord aan te passen naar een eigen wachtwoord. Let op dat dit wachtwoord goed onthouden wordt, aangezien het token zichzelf zal vergrendelen bij meermaals foutief invoeren. Een wachtwoordmanager is hiervoor aan te raden.

2a. Wachtwoord aanpassen bij SafeNet tokens

Volg onderstaande stappen om het tijdelijke wachtwoord van een SafeNet token aan te passen;

1. Start de SafeNet Authentication Client Tools software op.
2. Steek het token in de computer.
3. Klik in de SafeNet Authentication Client Tools applicatie bovenaan op het tandwiel icoon.
4. Klik met de rechtermuisknop op het 1e item onder ‘tokens’, vermoedelijk ‘Ensure e-Sign USB’ en kies voor ‘Change Password …’
5. Vul nu het tijdelijke wachtwoord in bij ‘Current Token Password’ en het gewenste nieuwe password in de twee onderste velden.
6. Klik op ‘OK’ om het nieuwe wachtwoord in te stellen.

2b. Wachtwoord aanpassen bij Feitian tokens - Windows

Volg onderstaande stappen om het tijdelijke wachtwoord van een Feitian token aan te passen;

1. Start de Feitian Manager applicatie op.
2. Sluit het USB-token aan op jouw Windows-machine.

3. Druk na een paar seconden op **Control + Alt + Delete.**
4. Selecteer **Wachtwoord wijzigen** in de lijst met gepresenteerde opties.
5. Klik op **Aanmeldingsopties** net boven de knop Annuleren.
6. Klik op het pictogram **Smartcard** naast het sleutel pictogram.
7. Je ziet nu het token type en velden voor oude en nieuwe pincode.
8. Voer het oude (tijdelijke) wachtwoord in het eerste veld in.
9. Voer het nieuwe wachtwoord in het 2e veld in en herhaal dit wachtwoord in veld nr. 3.
10. Klik op de pijl naar rechts in het derde veld om het nieuwe wachtwoord op te slaan.

2c. Wachtwoord aanpassen bij Feitian tokens - MacOS

Volg onderstaande stappen om het tijdelijke wachtwoord van een Feitian token;

1. Steek het token in één van de USB poorten van jouw Mac
2. Open de 'EnterSafeCastleAdminMgr.app' applicatie vanuit de Applicatie folder.
3. Klik op de **Change User PIN** knop onderin het venster.
4. Vul het ingestelde, tijdelijke wachtwoord in bij veld 1.
5. Vul het nieuwe wachtwoord in bij veld 2 en 3.
6. Klik op **OK** om het nieuwe wachtwoord op te slaan.

3. Downloaden certificaat bestanden

Het bestelde certificaat zal pas worden uitgegeven wanneer de toegezonden verificatiecode via het Ensured collection formulier wordt verzonden. Hiervoor is een apart email bericht afkomstig van ensured.com verzonden aan het email adres welke is opgegeven tijdens de bestelling. In dit bericht staat een unieke URL vermeld, samen met een Verificatiecode. Zodra de Verificatiecode is ingevuld en op de knop 'Haal op' wordt gedrukt zal het certificaat worden aangemaakt en volgt na een tiental seconden de download in vorm van een 'certificate.cer' bestand.

Samen met het eigen certificaat zullen ook de zogenoemde CA certificaten op het token geïnstalleerd moeten worden, je kunt deze apart downloaden via onderstaande URL;

https://www.ensured.nl/support/Ensured_Downloads/Ensured_Root_certificaten

4. Installatie certificaat bestanden op token

Nadat je het nieuwe certificaat hebt gedownload, open je de beheersoftware van Feitian of Safenet, afhankelijk van het type token dat je bij je bestelling hebt ontvangen. Volg de stappen bij 4a voor de SafeNet tokens, of 4b wanneer je een Feitian token hebt ontvangen.

4a. Installatie certificaat op Safenet tokens

1. Open de Safenet Authentication Client Tools applicatie.
2. Selecteer de **geavanceerde weergave** door op het tandwielpictogram te klikken.
3. Selecteer je token aan de linkerkant.
4. Klik op het import pictogram.
5. Voer het wachtwoord in om het token te ontgrendelen.
6. Klik op de knop **Bladeren** en selecteer het .cer-bestand dat is gedownload van het Ensured collection formulier; jouw pdf-certificaat.
7. Klik nogmaals op **importeren**.
8. Klik op de knop **Bladeren** en selecteer het bestand 'EnsuredRootCA.cer' dat is gedownload van de Ensured-website.
9. Klik op **OK** om het certificaat te importeren.
10. Klik nogmaals op **importeren**.
11. Klik op de knop **Bladeren** en selecteer het bestand 'EnsuredDocumentSigningCA.cer' dat is gedownload van de Ensured-website.
12. Klik op **OK** om het certificaat te importeren.

4b. Installatie certificaat op Feitian tokens

1. Open de ePass Manager-applicatie.
2. Voer het wachtwoord in om het token te ontgrendelen.
3. Klik op **importeren**.
4. Klik op de knop **Bladeren** en selecteer het .cer-bestand dat is gedownload van het Ensured collection formulier; jouw pdf-certificaat.
5. selecteer de optie * **Handtekening *** onderaan dit venster en klik op **OK** om het certificaat te importeren. Deze stap is belangrijk omdat anders het certificaat niet zichtbaar zal zijn in Acrobat.
6. Klik nogmaals op **importeren**.
7. Klik op de knop **Bladeren** en selecteer het bestand 'EnsuredRootCA.cer' dat is gedownload van de Ensured-website.
8. Klik op **OK** om het certificaat te importeren.
9. Klik nogmaals op **importeren**.
10. Klik op de knop **Bladeren** en selecteer het bestand 'EnsuredDocumentSigningCA.cer' dat is gedownload van de Ensured-website.
11. Klik op **OK** om het certificaat te importeren.

Nu is je token klaar om te worden geconfigureerd met je PDF-applicatie. Let op:

- Het certificaat en de persoonlijke sleutel zijn op het token geïnstalleerd en kunnen niet worden geëxporteerd.
- Het is mogelijk om het token op meerdere machines te gebruiken, maar slechts één tegelijk.

Als deze stap is voltooid, kun je je certificaat gebruiken!

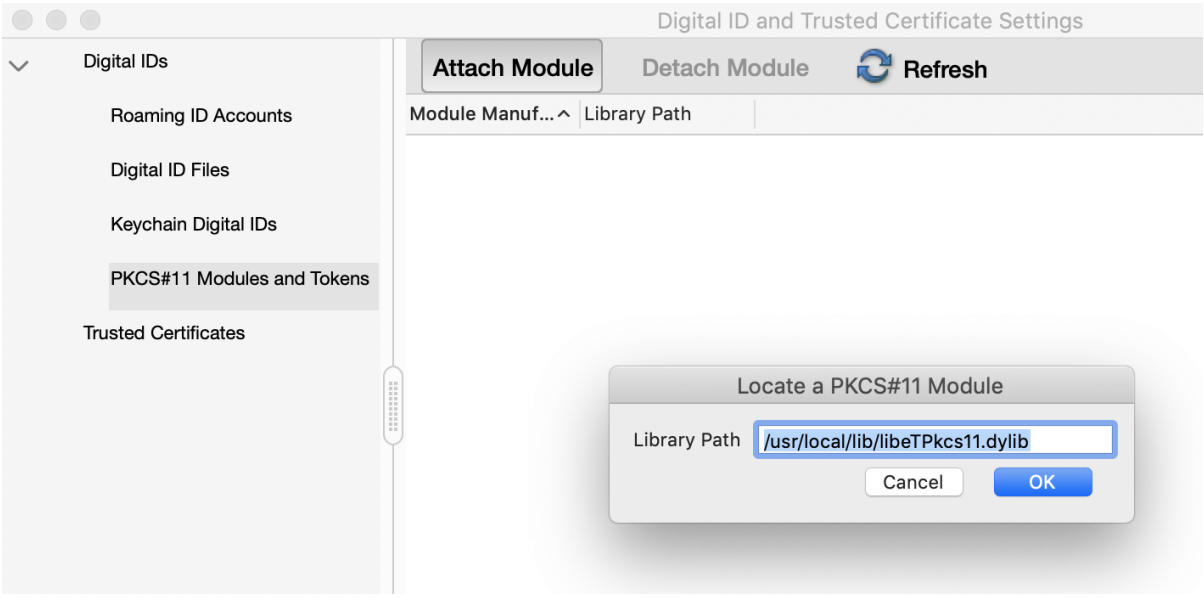
5. Configuratie Adobe Acrobat

De Ensured PDF handtekening wordt standaard vertrouwd in Adobe Reader door opname in de Adobe AATL lijst. Daarnaast kun je Adobe ook gebruiken voor het ondertekenen en/of tijdstempelen van PDF documenten.

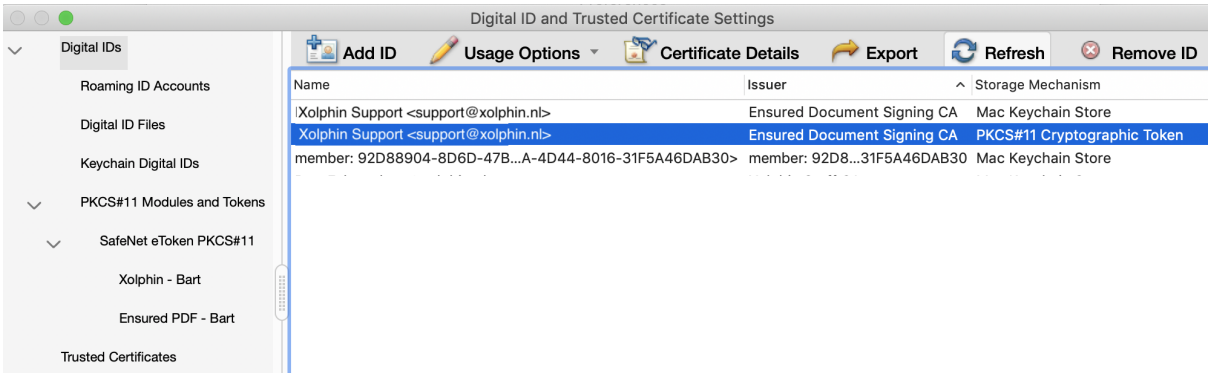
Deze handleiding is van toepassing op Adobe Acrobat Pro DC (versie 2019.012.20034) en Adobe Acrobat Reader DC (versie 2019.012.20034) en latere versies. Voorafgaand aan deze configuratie moeten de juiste drivers geïnstalleerd worden zoals beschreven in stap 1 van deze handleiding.
Laat het token gedurende onderstaande processen in de machine zitten.

Configuratie van een PDF signing certificaat in Adobe Acrobat

1. Start Adobe Acrobat.
2. Open het Voorkeuren venster (Windows: CTRL+K of Mac: ⌘ + ,).
3. Selecteer de categorie **Handtekeningen.**
4. Klik op **Meer...** onder de categorie **Identiteiten & vertrouwde certificaten.**
5. Klik op **Digitale ID's > PKCS#11 Modules en Tokens.**
6. Klik op **Module koppelen.**
7. Voer het pad in naar PKCS#11 library, dit is (als de aangeraden drivers geïnstalleerd zijn).Voor **Feitian** tokens;
    - Op de Mac is het pad; **/usr/local/lib/libcastle.1.0.0.dylib**
    - Voor Windows is het pad; **C:\Windows\system32\eps2003csp11.dll**
8. Voor **Safenet** tokens;
    - Op de Mac is het pad; **/usr/local/lib/libeTPkcs11.dylib**
    - Voor Windows is het pad; **C:\Windows\system32\eToken.dll**



9. Na het invoeren van het pad naar de driver, klik op 'Ok' om het token te activeren.
10. Klik het juiste token aan onder PKCS#11 Modules and Tokens aan de rechterkant, klik op **Aanmelding,** voer het token wachtwoord in en klik op **Ok**.
11. Klik nu op **Digitale ID's.**
12. Selecteer nu het certificaat met het Storage mechanism: **PKCS#11 Cryptographic Token.**



13. Klik nu op **Gebruiksopties** *(potlood)***.**
14. Selecteer nu **Gebruiken voor ondertekenen** (of in Acrobat Pro **Use for Certifying**).
15. Er verschijnt nu een pen of een rozet voor de naam van het geselecteerde certificaat.
16. Klik op **Close** en in de onderliggende dialoog op **OK.**

Adobe Acrobat is nu geconfigureerd om handtekeningen te genereren met het certificaat dat geïnstalleerd staat op het token.

5b. Configuratie van een Timestamp Server in Adobe Acrobat

Door naast een digitale handtekening ook een tijdstempel (timestamp) aan een PDF document toe te voegen, blijft je ondertekening ook controleerbaar als je PDF certificaat niet meer geldig is.

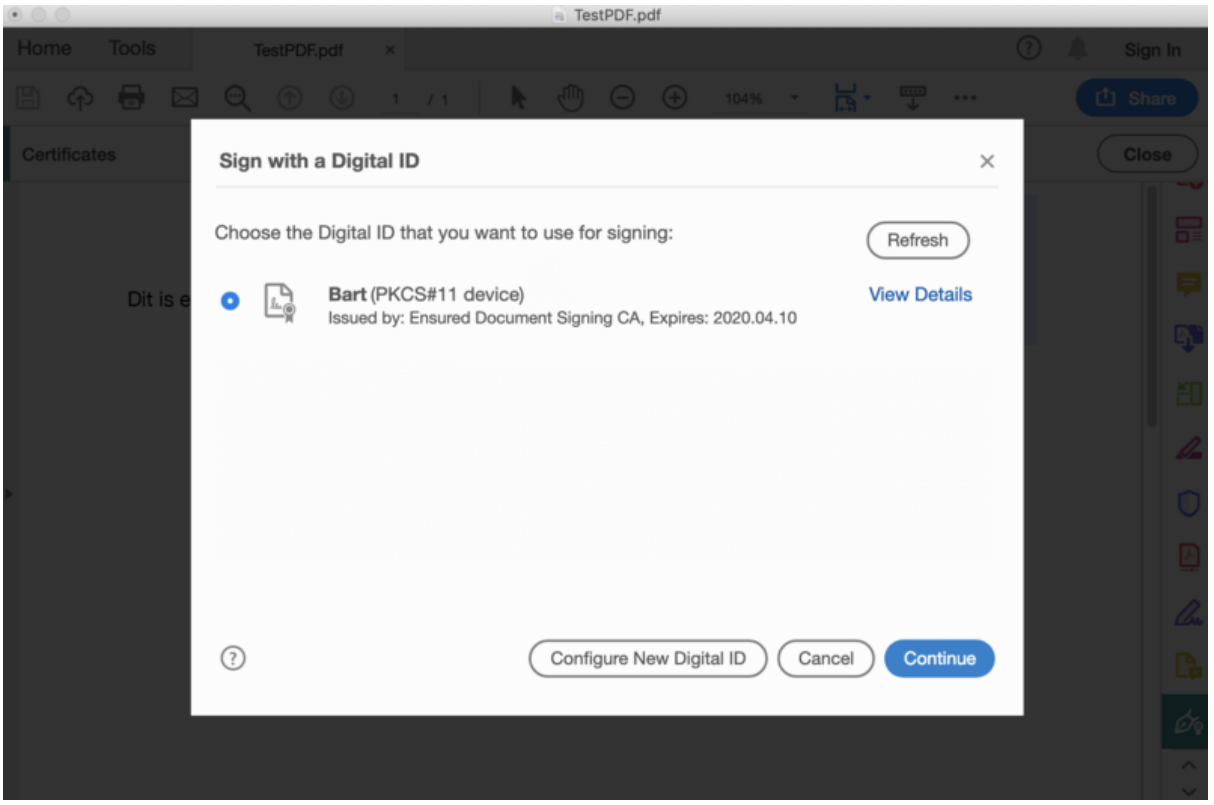
1. Start Adobe Acrobat.
2. Open het Preferences venster (⌘ + ,).
3. Selecteer de categorie **Handtekeningen.**
4. Klik op **Meer...** onder de categorie **Tijdstempel voor document.**
5. Klik op **Nieuw.**
6. Voer een naam in (bv. Timestamp server) en de server URL (voor Ensured: http://timestamping.ensuredca.com)
7. Klik op **OK.**
8. Selecteer de toegevoegde Timestamp Server en klik op **Standaard instellen.**
9. Klik op **Close** en in de onderliggende dialoog op **OK.**

Adobe Acrobat is nu geconfigureerd om tijdens het zetten van de handtekening ook een timestamp te genereren.

6. Plaatsen van je eerste digitale handtekening

6a. Gebruik van een PDF signing certificaat in Adobe Acrobat

1. Start Adobe Acrobat en open een PDF-document.
2. Klik in het menu op **Bewerken** en dan **Gereedschappen beheren.**
3. Klik op **Certificaten.**
4. Bovenaan verschijnt nu een extra balk, klik hier op **Digitaal ondertekenen** (of in Acrobat Pro op **Certify**).
5. Teken het gevraagde **Handtekening kader** ergens in het document.
6. Selecteer nu het certificaat met de juiste naam en waar achter de naam **(PKCS#11 device)** staat en klik op **Doorgaan.**



7. Pas nu eventueel de weergave van de handtekening aan, voer het token wachtwoord in en klik op **Ondertekenen.** Let op: het is ook mogelijk meerdere templates op te slaan voor handtekening weergave.
8. Sla het PDF-document op.

Het PDF-document is nu voorzien van een ondertekening. Als er een Timestamp Server is geconfigureerd als 'Default' zal deze Timestamp Server automatisch gebruikt worden om een timestamp te genereren voor het PDF-document. Deze timestamp wordt opgenomen in de ondertekening.

6b. Gebruik van een Timestamp Server in Adobe Acrobat

Het apart zetten van een timestamp is alleen nodig wanneer de Tijdstempel server niet als standaard staat ingesteld (zie punt 5b)

1. Start Adobe Acrobat en open een PDF-document.
2. Klik in het menu op **Bewerken** en dan **Gereedschappen beheren.**
3. Klik op **Certificaten.**
4. Bovenaan verschijnt nu een extra balk, klik hier op **Tijdstempel** (of als de Timestamp Server staat ingesteld als 'Default', klik op Digitally Sign).
5. Sla het PDF-document op.

6c. Meerdere handtekeningen toevoegen in Adobe Acrobat

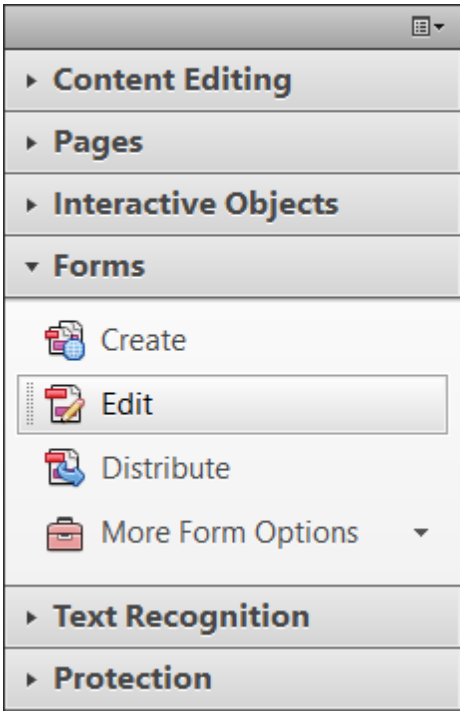
Het is mogelijk om meerdere handtekeningen toe te voegen aan een PDF document. Hiervoor is het nodig om ieder handtekening veld te plaatsen voordat er gestart wordt met ondertekenen. En terwijl het plaatsen van handtekeningen ondersteund wordt door Adobe Reader of Adobe Acrobat, ondersteunen alleen Adobe Acrobat Standard & Professional het plaatsen van handtekening velden.

Bij een workflow met meerdere handtekeningen gebruik je zowel de **Certify (Visible)** optie en de **Sign With Certificate** optie die beschikbaar zijn in Adobe Reader & Adobe Acrobat. De eerste handtekeningen gebruiken de ‘certify’ optie, omdat deze het mogelijk maakt na ondertekening meerdere handtekeningen te plaatsen. Alleen voor de laatste handtekening op het document gebruik je de ‘Sign with Certificate’ option, zodat hierna geen aanpassing of ondertekening meer mogelijk is. Bijvoorbeeld als je 5 handtekeningen wilt plaatsen, gebruiken de eerste vier de ‘certify’ optie en de vijfde de ‘Sign with certificate’ optie.

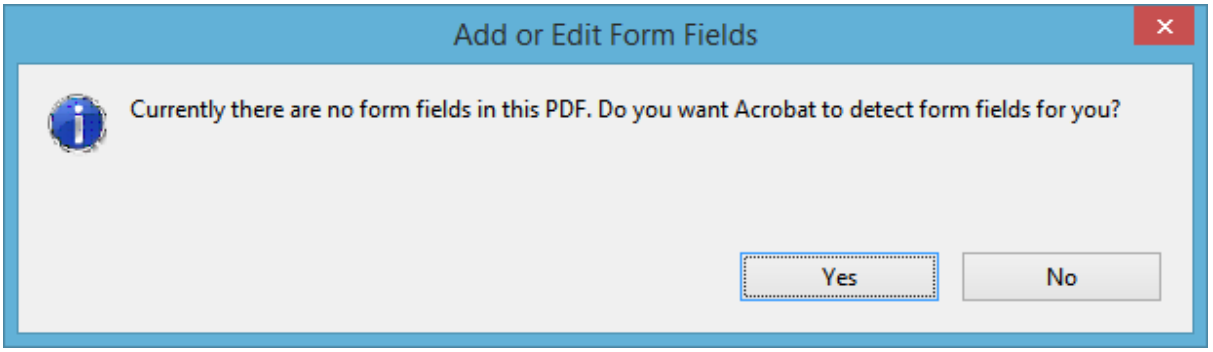
Handtekening velden toevoegen

1. Open Adobe Acrobat
2. Klik op het **Tools** menu boven rechts.

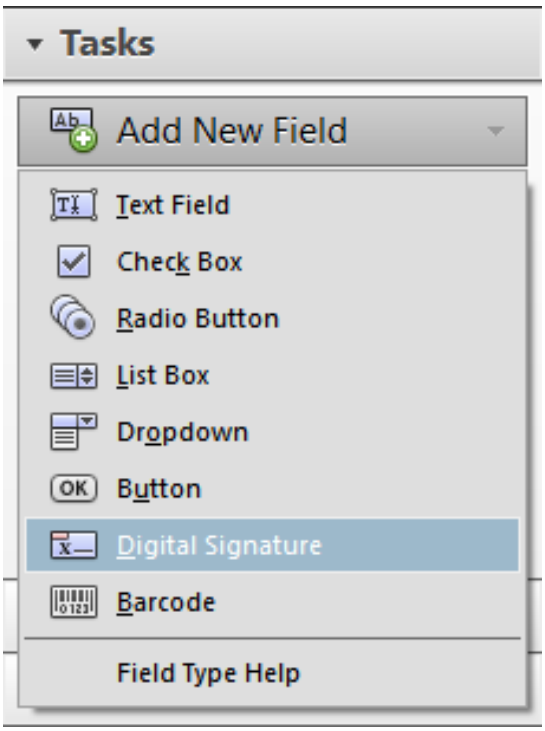
3. Klap het **Forms** gedeelte uit en klik op **Edit**.



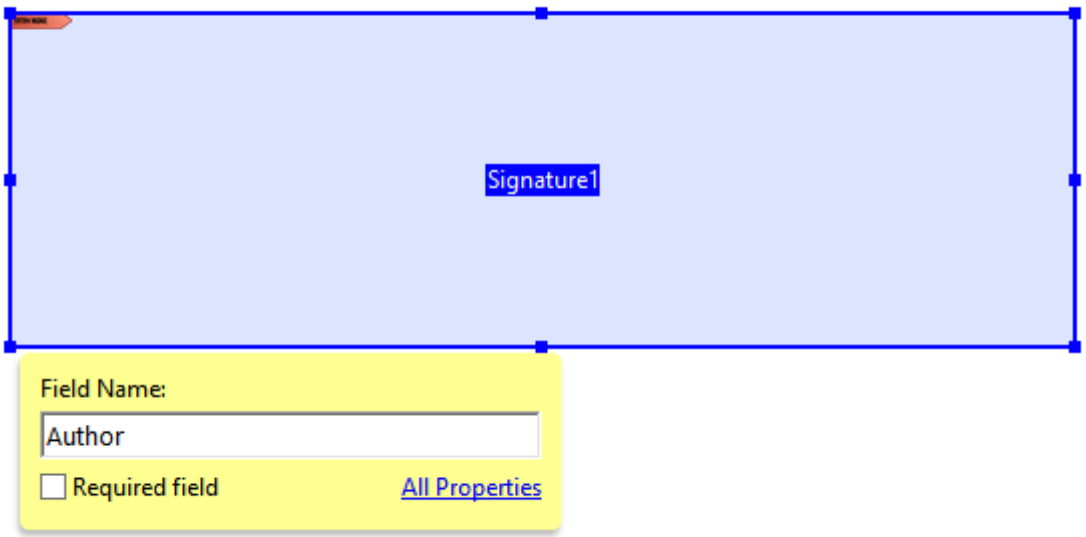
4. Bij de vraag voor het automatisch detecteren van formuliervelden, kies **No**.



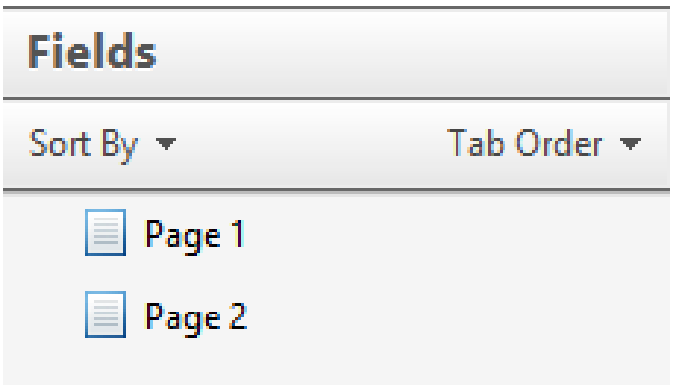
5. Bij de **Tasks** sectie, klik op **Add New Field** > **Digital Signature**.



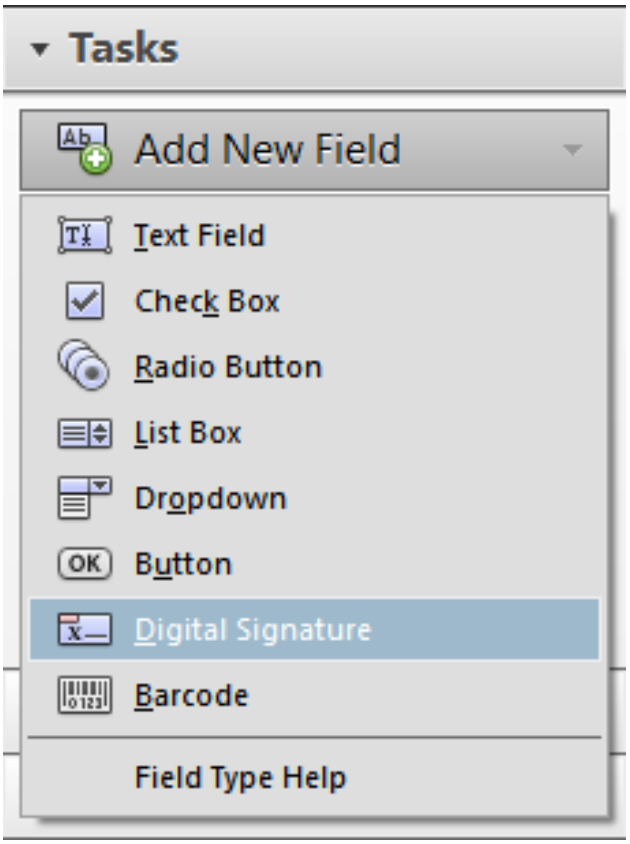
6. Sleep een rechthoek voor het creëren van de gewenste afmeting van het handtekeningveld. Je kunt optioneel een label voor de ondertekenaar toevoegen (bijvoorbeeld auteur, goedkeurder, getuige, etc).



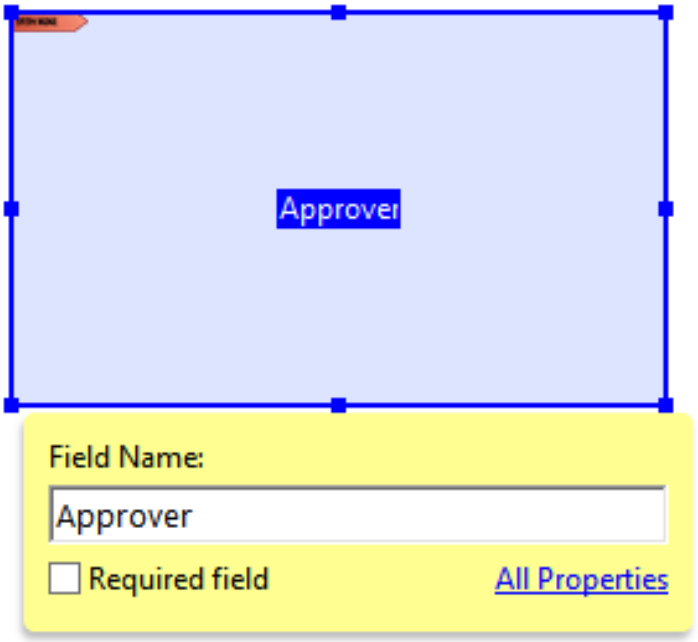
7. Als je PDF meerdere pagina's bevat, en de volgende handtekening komt op een andere pagina, klik dan op die pagina onder **Fields** om naar die pagina te gaan.



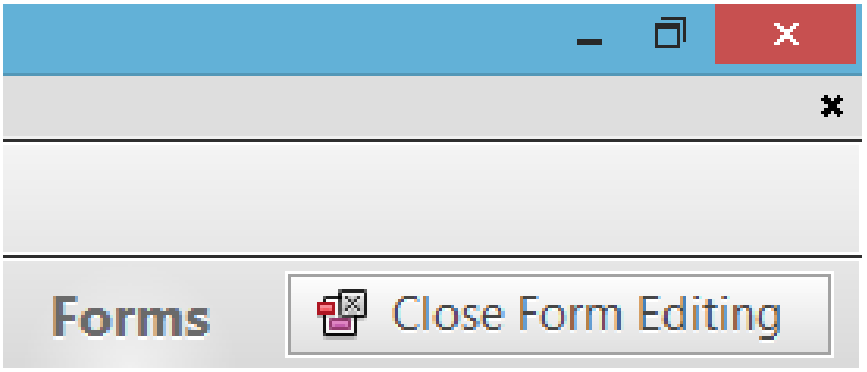
8. Nogmaals onder de sectie **Tasks**, klik op **Add New Field** > **Digital Signature**.



9. Sleep nogmaals een rechthoek voor het plaatsen van een volgend handtekeningveld, en label het weer (optioneel) voor de beoogde ondertekenaar.



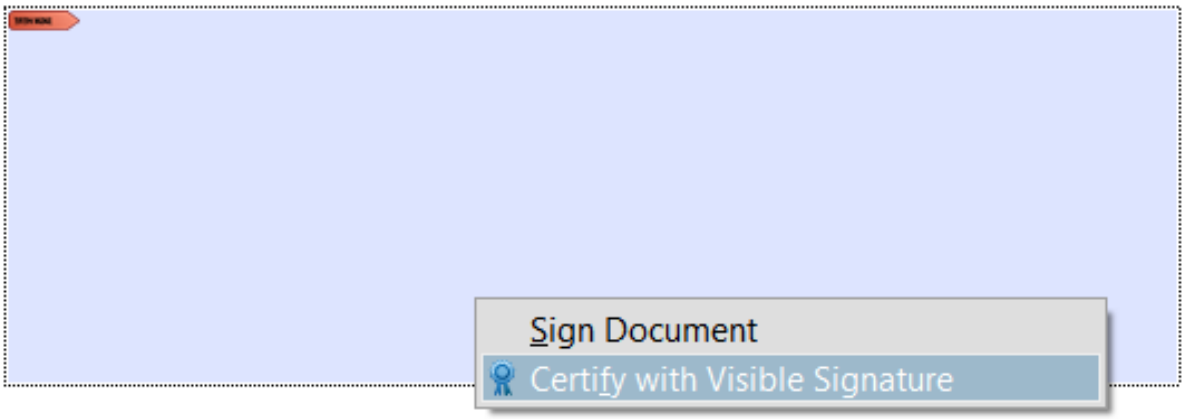
10. Herhaal dit proces totdat alle handtekeningvelden geplaatst zijn.
11. Klik hierna op **Close Form Editing** om de formulier bewerker te sluiten.



12. Sla de PDF op; het document is nu gereed voor ondertekening.

Meerdere handtekeningen plaatsen

Open een PDF die meerdere handtekening velden bevat. Klik met de rechtermuisknop het eerste handtekeningveld en kies voor **Certify with Visible Signature**.



1. Het **Certify Document** venster verschijnt nu.
2. Als je meerdere certificaten hebt, kies je het gewenste certificaat via het **Sign As:** drop-down menu.
3. Pas de weergave van de handtekening aan zoals je dat wilt.
4. Zorg er bij **Permitted Actions After Certifying** voor dat of **Form fill-in and digital signatures** of **Annotations, form fill-in, and digital signatures** is geselecteerd zodat het mogelijk is extra handtekeningen te plaatsen..
5. Klik **Sign.**
6. Bewaar de PDF & vul het wachtwoord in voor jouw certificaat/USB Token.

De volgende stappen hangen af van het aantal handtekeningen, of of deze door een persoon of door meerdere personen worden geplaatst. Als de volgende handtekening door een ander persoon gezet moet worden, stuur dan het gecertificeerde document door. Als je zelf meerdere handtekeningen wilt plaatsen, selecteer je het volgende handtekeningveld, gevolgd door **Certify with Visible Signature.**

Zodra de laatste handtekening wordt toegevoegd:

1. Klik op het handtekening veld om het **Sign Document** venster te openen.
2. Selecteer je certificaat bij de **Sign As:** drop-down.
3. Pas de weergave van de handtekening naar jouw voorkeur aan.
4. Vink het vakje **Lock Document After Signing** aan.
   Let op: een niet gelocked kan niet inhoudelijk aangepast worden, wel is het hierbij toegestaan invulvelden te vullen en te ondertekenen. Na het locken van een document is dit ook niet meer mogelijk.
5. Klik op **Sign** .
6. Bewaar de PDF & vul het wachtwoord voor jouw certificaat/USB token in.

Het document bevat nu de laatste handtekening. Alle certificeringen en handtekeningen zouden nu geldig en individueel te valideren moeten zijn via het handtekeningen venster.