HANDLEIDING : Beveiliging en controle van de PDF-documenten

De documenten zijn gecertificeerd door Belfius Bank aan de hand van een certificaat afgeleverd door Certipost.

De handtekening garandeert volgende zekerheden :

- **Integriteit:** gaat het zeker om een niet gewijzigd origineel document ?

- **Authenticiteit**: Gaat het zeker om een origineel document afgeleverd door Belfius Bank ? De controle wordt gerealiseerd door middel van een root-certificaat. Zo ismen zeker van de authenticiteit van de handtekening.

- **Niet revocatie:** Is het certificaat gebruikt voor de handtekening niet gerevoceerd (geannuleerd) en nog steeds geldig op het ogenblik van gebruik ?

Om deze 3 controle zekerheden te kunnen gebruiken, is het nodig éénmalig een root certificaat te installeren op uw PC.

Voor de controle van de elektronische handtekening is versie 7 of hoger vereist van ADOBE READER. Het gebruik van een lagere versie resulteert in een foutmelding. Wij raden aan om gratis de meest recente versie van ADOBE READER te installeren via de website www.adobe.be.

Om het certificaat te installeren kunnen er twee procedures worden gevolgd. U kan naar keuze de stappen volgen van hoofdstuk 1 of van hoofdstuk 2.

Opmerking: De schermen en de terminologie van Windows- en Adobe-software weergegeven in dit document zijn afkomstig uit de Nederlandstalige versie.
Indien u beschikt over een anderstalige versie is de terminologie verschillend maar de te volgen procedure is identiek.

Hoofdstuk 1

INSTALLATIE via WINDOWS & CONFIGURATIE VAN ADOBE READER

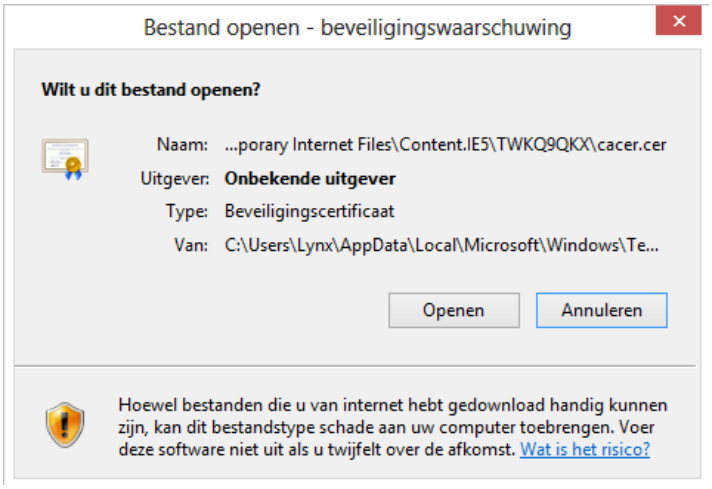
1.1. Installatie vanuit WINDOWS

- Het 'root-certificaat' is beschikbaar :

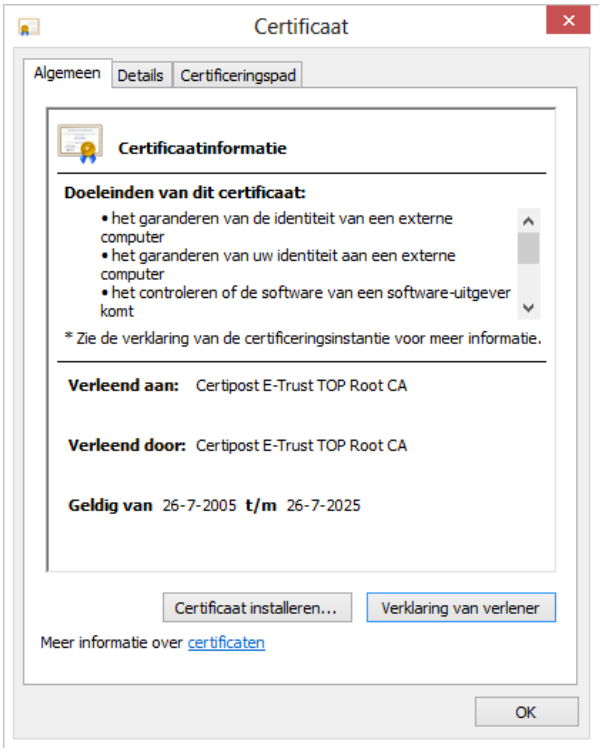
- Rechtstreeks op de site van Certipost. (onafhankelijke bron)
  http://certipost.be/download/trust/certs/cacer.crt

- Er verschijnt een venster met de vraag of U het bestand wenst te openen («Openen») of op te slaan (« Opslaan »). Kies « Openen ».

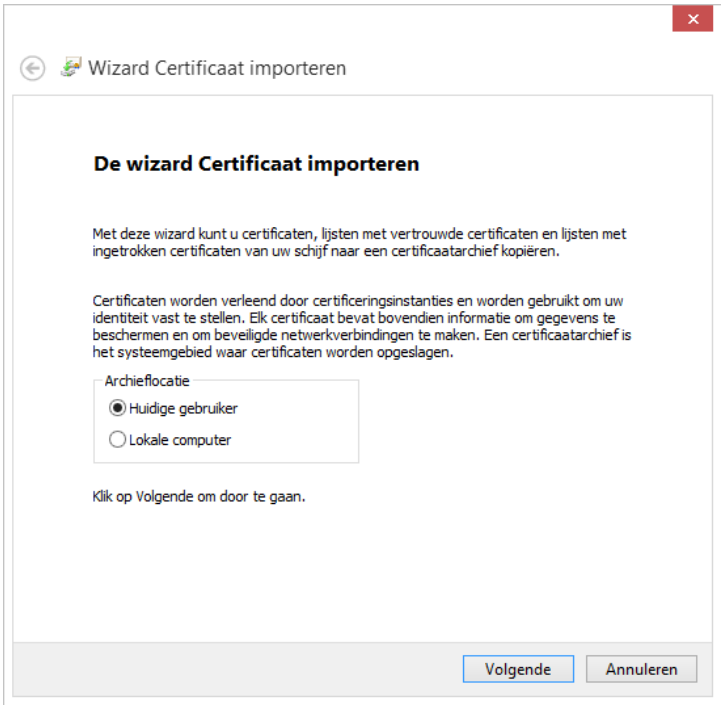
-Kies nogmaals « Openen ».



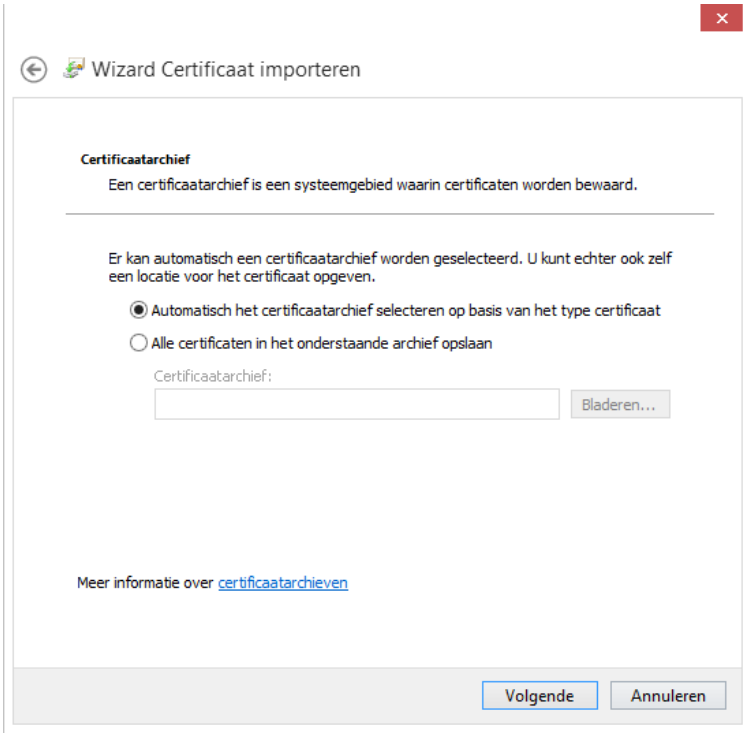
Er verschijnt een venster dat de eigenschappen van het certificaat toont. Klik op de knop « CERTIFICAAT INSTALLEREN ».



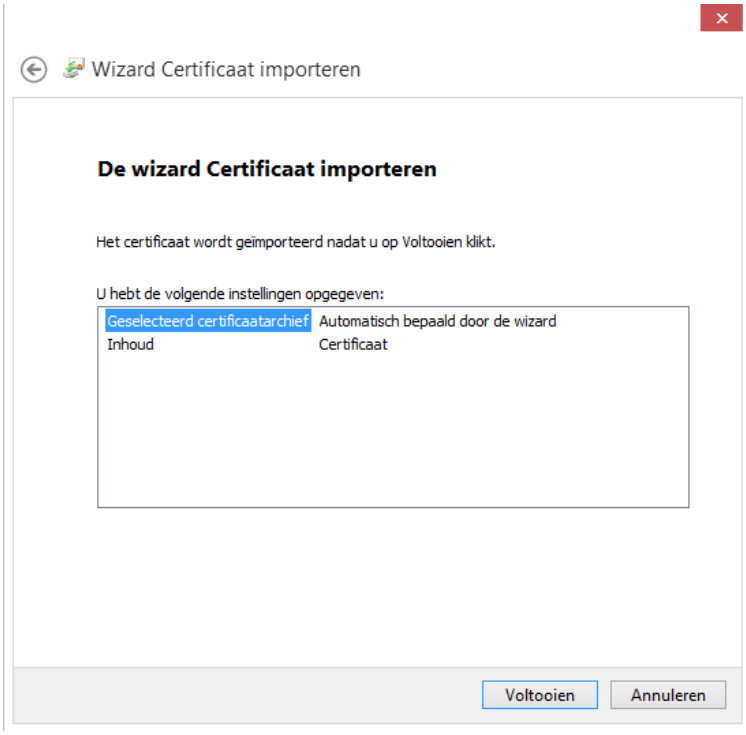
Er verschijnt een venster met de wizard voor certificaten te importeren, kies voor « Huidige gebruiker », (tenzij u administrator bent van uw pc, dan kiest u voor «Lokale computer »), nadien klikt u op «Volgende ».



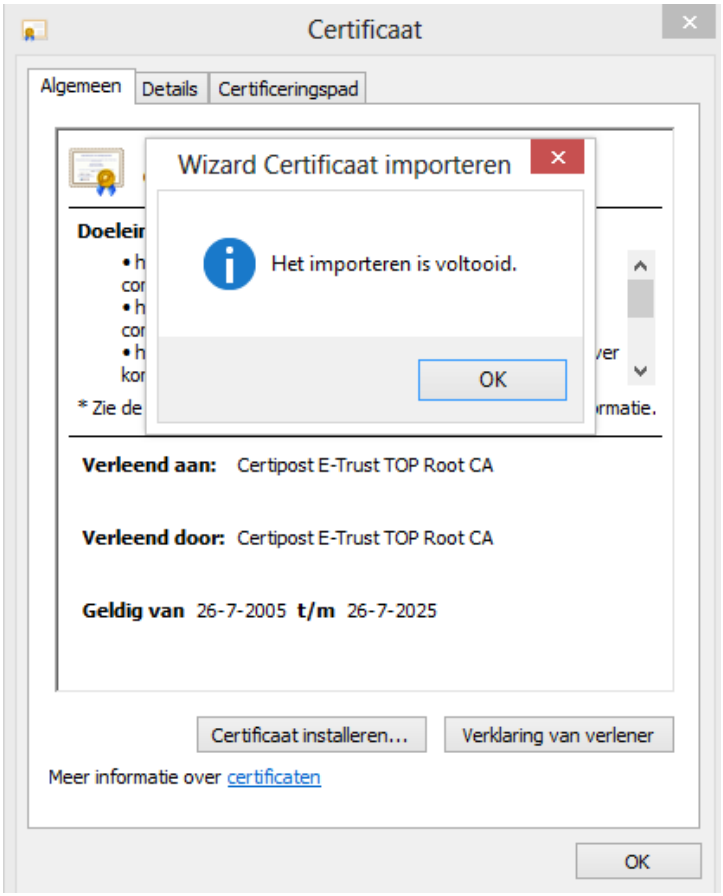
Het volstaat om vervolgens de voorgestelde optie te bevestigen , kies «Volgende »



en vervolgens «Voltooien»



U krijgt een bevestiging van het geïmporteerde certificaat , klik hierop «OK»

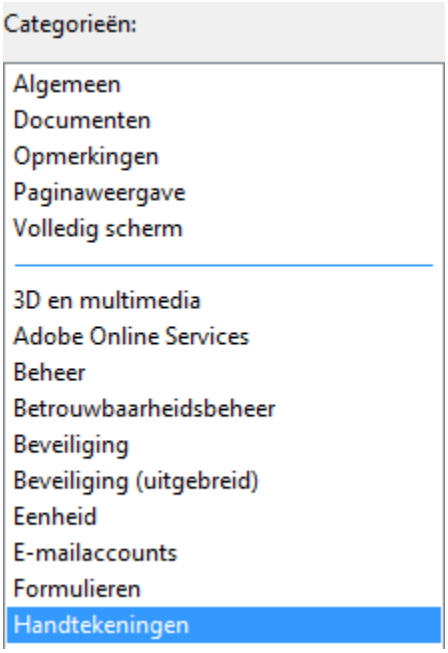


Via deze procedure is het certificaat geïnstalleerd in de ‘root-store’ van Windows.
Met de tweede stap wordt vervolgens de toepassing ADOBE toestemming gegeven om het certificaat te gebruiken

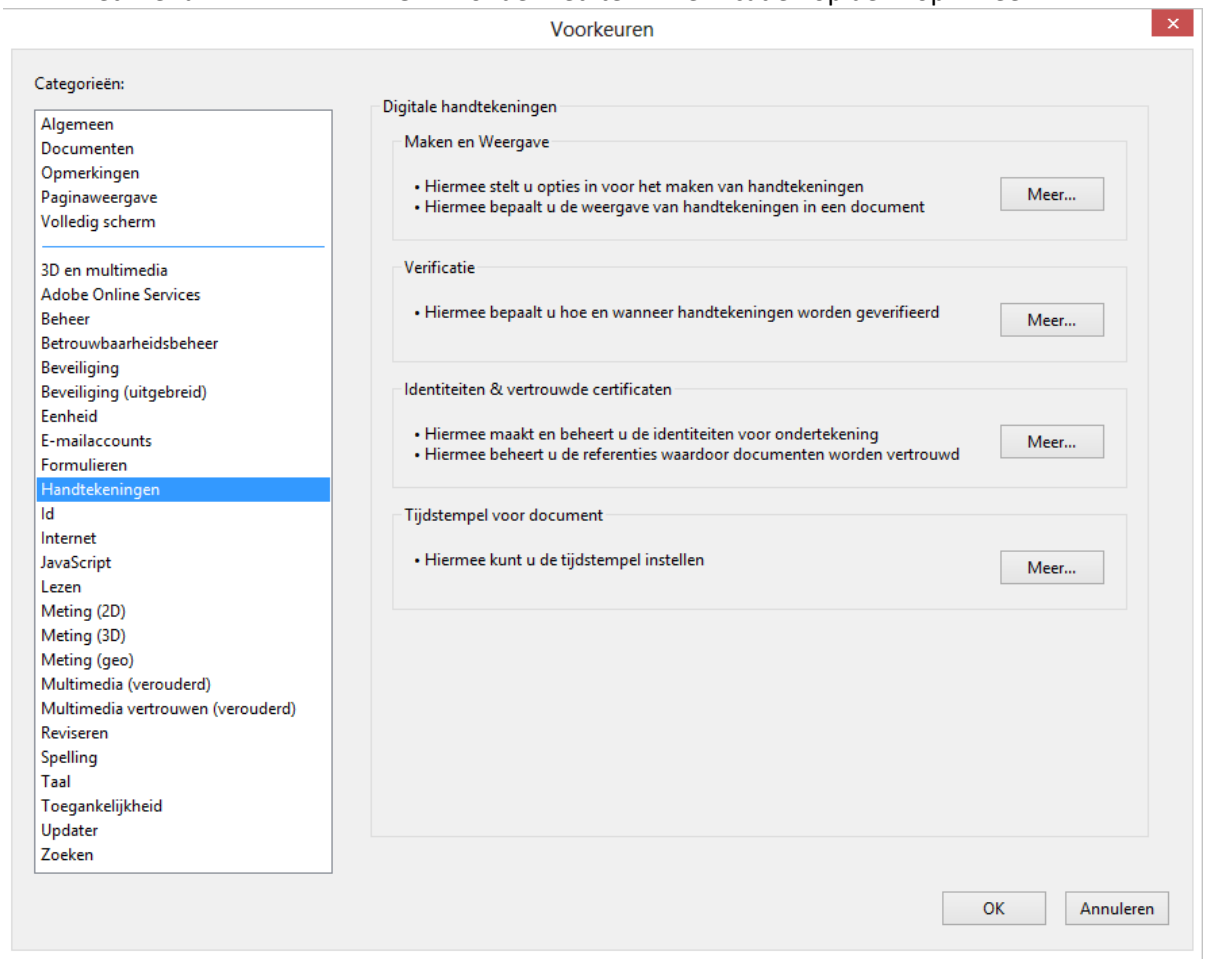
1.2. Configuratie van de toepassing ADOBE

Open Adobe Reader en kies het menu «BEWERKEN»- «VOORKEUREN»

In voorkeuren , onder categorieën selecteert u «HANDTEKENINGEN»



Klik in het Menu «HANDTEKENINGEN» onder het item «Verificatie» op de knop «Meer»



Onder de voorkeuren voor handtekeningverificatie ,
Klik op de knop «Meer» onder het item «Verificatie»

- **Onder het menu «Verificatiegedrag», de volgende optie UITVINKEN**
  "Wanneer mogelijk succesvolle controle op certificaatintrekking vereisen bij verificatie van handtekeningen"

  Geeft aan of de controle van niet-revocatie moet worden uitgevoerd. Deze connectie wordt uitgevoerd via het internet (de pc moet geconnecteerd zijn aan het internet)en vraagt enige tijd. Gezien de beperkte toegevoegde waarde van deze controle en de afhankelijkheid van internet, bent u vrij deze optie al dan niet te activeren.

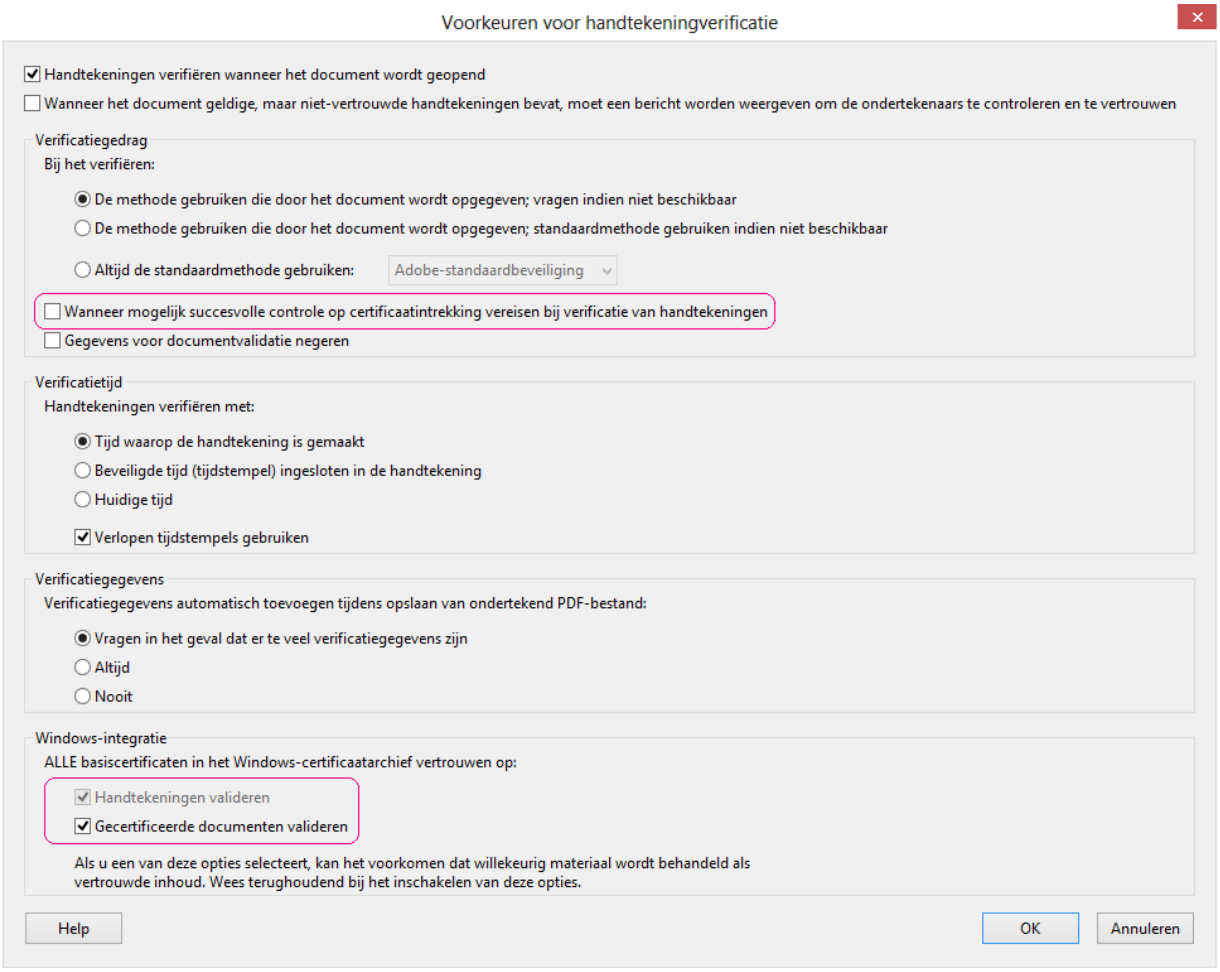
  Bijkomende opmerking (enkel als de hierboven vermelde optie geactiveerd is).
  De CRL controle gebeurt via het Internet: Als uw internettoegang via een proxy gebruikt wordt, moet u ook zorgen dat die proxy correct ingesteld is om die CRL controle toe te laten. Contacteer hiervoor uw netwerkbeheerder. Hij moet ervoor zorgen dat

a) er geen «caching» van de crl's gebeurt
b) er geen authentificatie of een http/1.0. authentificatie op de website van certipost is.

De niet-revocatie controle is nodig om te kunnen verifiëren dat het certificaat dat Belfius Bank gebruikt voor het plaatsten van de digitale handtekening niet werd gerevoceerd. Een certificaatrevocatie is –in het geval van PaPyRuS- puur theoretisch. Die certificaten zijn inderdaad op beveiligde apparatuur geïnstalleerd en hebben bovendien geen enkele commerciële waarde (die worden enkel gebruikt voor het tekenen van onze reporting documenten). Het risico dat dit certificaat ooit "gestolen" wordt is nihil en dit certificaat zou nooit op de CRL lijst mogen komen (lijst van gerevoceerde certificaten)

- **Onder het menu Windows-integratie beide opties AANVINKEN**

U hebt via stap 1 het certificaat in Windows geïnstalleerd. Maar omdat de controle via ADOBE gebeurt, moet men in ADOBE vermelden dat de in WINDOWS geïnstalleerde certificaten gebruikt mogen worden. Omdat de parameters per pc worden bewaard, moeten deze slechts één maal gedefinieerd worden. De gekozen regels worden toegepast bij het openen van het volgende document. Indien een document al geopend is, kan men dit opnieuw controleren. Hiervoor dient men rechts te klikken op het icoontje van de handtekeningen en de optie '**Validate Signature**' kiezen.



Hoofdstuk 2

INSTALLATIE direct vanuit ADOBE.

(Enkel uit te voeren indien u de onder hoofdstuk 1 vermelde procedure niet heeft uitgevoerd).

Stap1

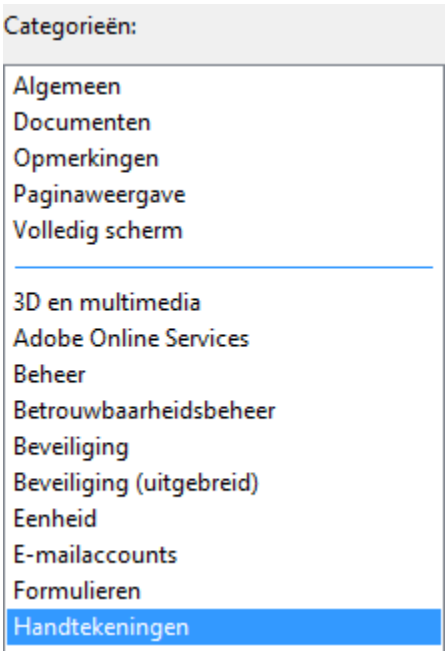
- Het 'root-certificate' is beschikbaar : Rechtstreeks op de site van Certipost. (onafhankelijke bron) http://certipost.be/download/trust/certs/cacer.crt

- Er verschijnt een venster met de vraag of U het bestand wenst te openen («Openen») of op te slaan (« Opslaan »). Kies « Opslaan ».

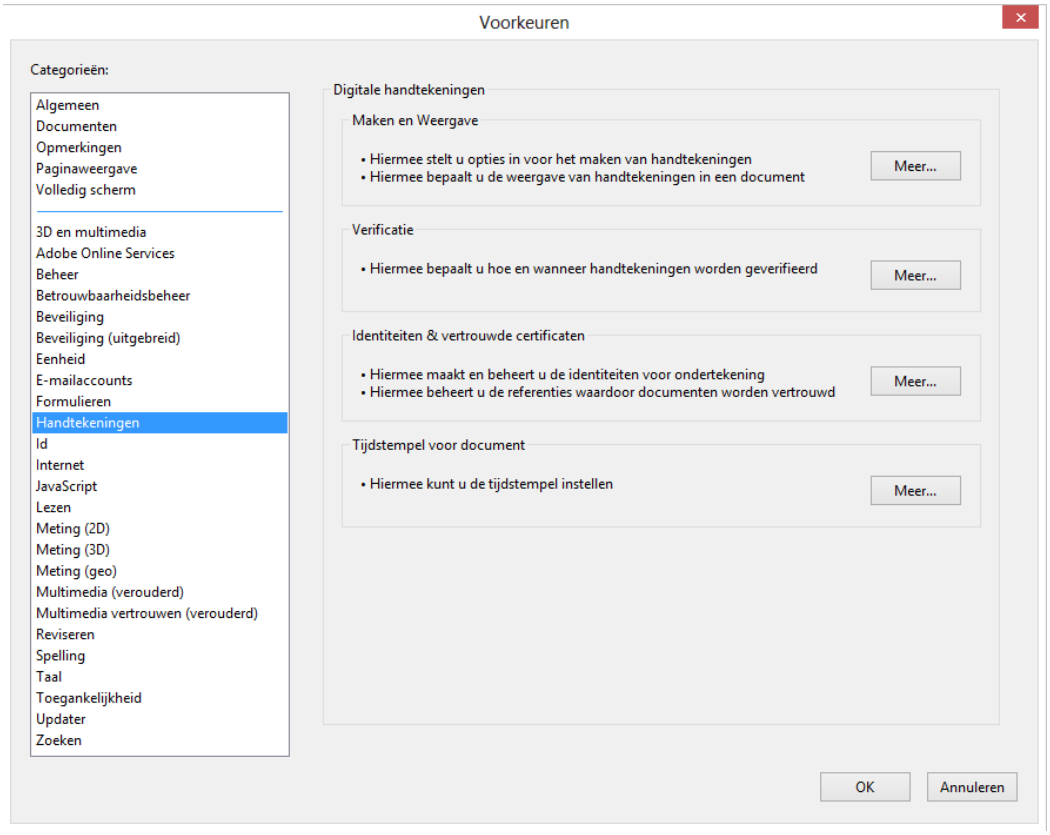
Duidt vervolgens aan waar het certificaat wordt opgeslagen (lokaal)

Stap 2

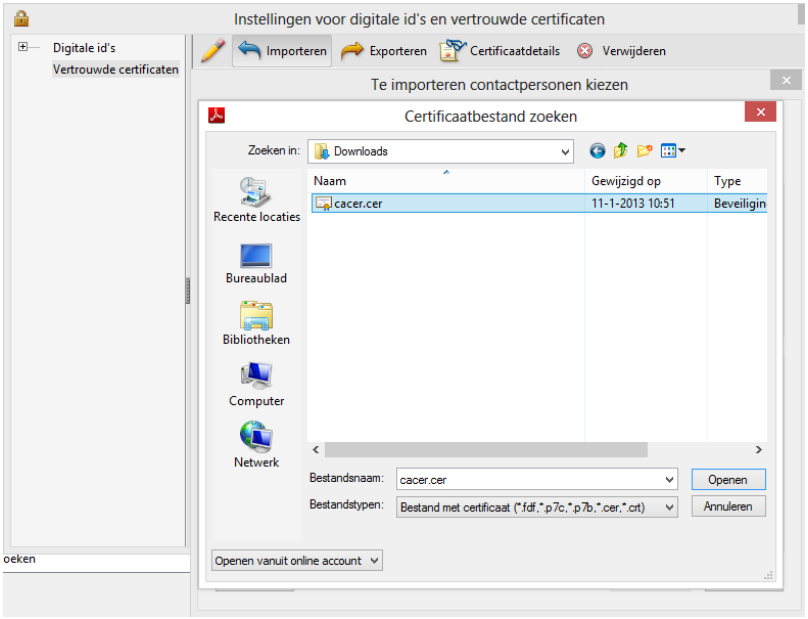
Open Adobe Reader en kies het menu «BEWERKEN»- «VOORKEUREN»
In voorkeuren , onder categorieën selecteert u «HANDTEKENINGEN»



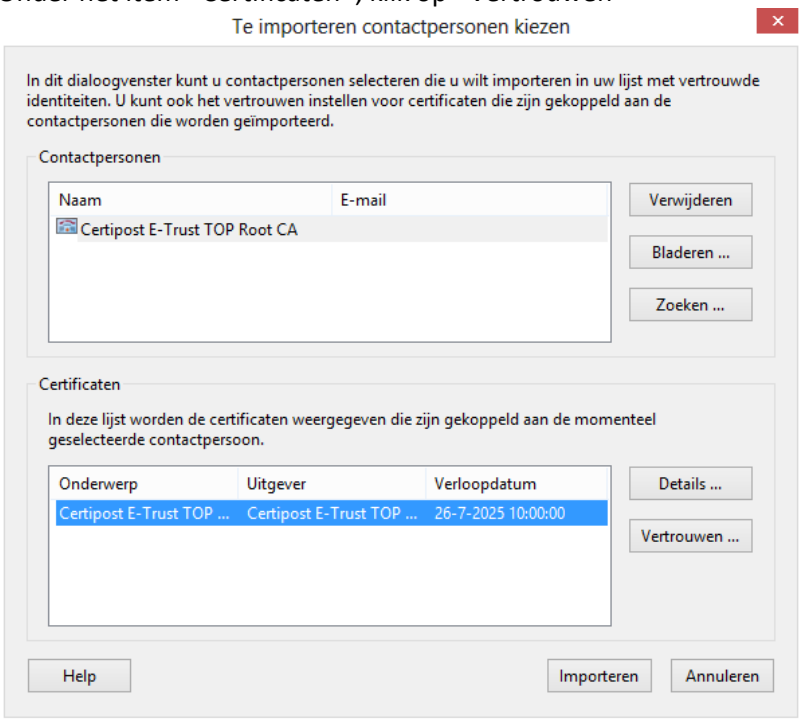
Onder de voorkeuren voor handtekeningverificatie , Klik op de knop «Meer» onder het item «Identiteit en vertrouwde certificaten»



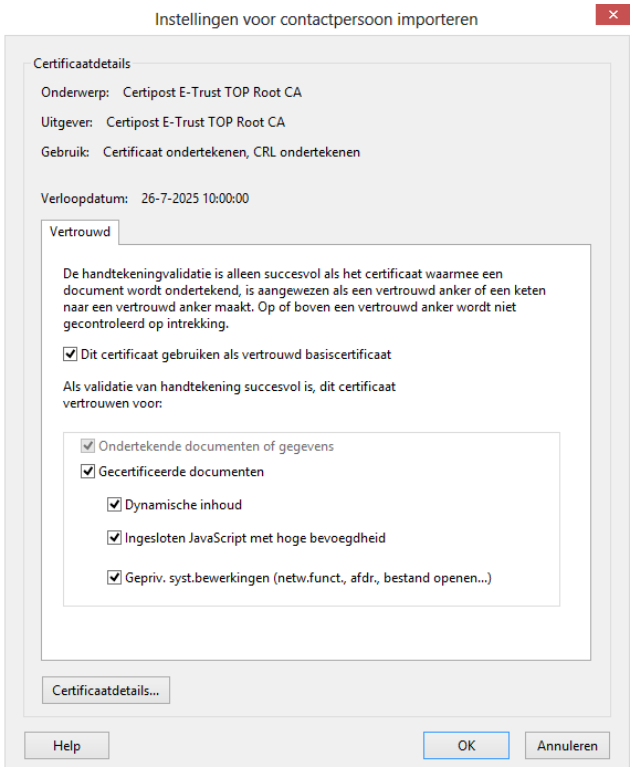
Kies in het linker menu voor «Vertrouwde certificaten», vervolgens kies in het menu bovenaan voor «Importeren», selecteer via «Bladeren» het opgeslagen certificaat(zie ***Stap 1***)
Selecteer het certificaat en klik op «Openen»



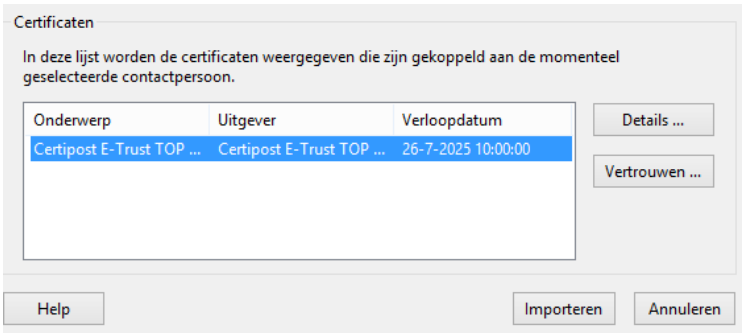
Onder het item «Certificaten», klik op «Vertrouwen»



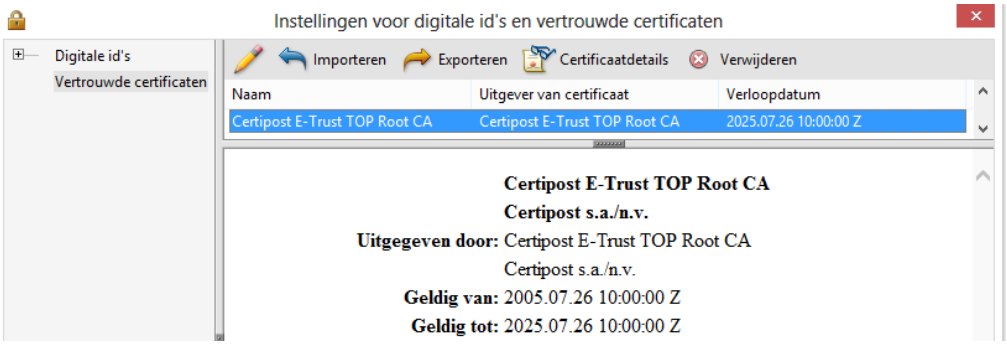
Bij de certificaatdetails activeer de optie «***Dit certificaat gebruiken als vertrouwd basiscertificaat***» en ook de bijhorende opties voor validatie activeren. Klik op «OK»



Vervolgens klikt u op «Importeren»



Het certificaat bevindt zich nu in de lijst van vertrouwde certificaten



Hoofdstuk 3.

HOE EEN GEOPEND DOCUMENT CONTROLEREN

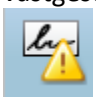
Eenmaal voorgaande opties zijn gedefinieerd, wordt elk geopend document automatisch gecontroleerd.

- Is het resultaat zoals in de afbeeldafbeelding hieronder, dan kan u uw document als volledig geldig en integer beschouwen.

- Is het resultaat zoals in afbeeldafbeelding hieronder, dan wil dit zeggen dat het systeem een fout heeft vastgesteld:

- Ofwel maakt u gebruik van een versie van Adobe die niet compatibel is (versie 6 of lager);
- Ofwel is het document gewijzigd na het plaatsen van de handtekening. In sommige gevallen kan de initiële versie van het documenten teruggevonden worden door rechts te klikken op de afbeelding van de handtekening en de optie 'View signed version' te selecteren.
U kan de originele versie van de documenten steeds verkrijgen via BelfiusWeb

- Is het resultaat zoals in afbeelding hieronder, dan werd bij de controle geen onregelmatigheid vastgesteld, maar is de identiteit van Belfius Bank niet bevestigd :



- Ofwel omdat het 'root-certificate' niet correct is geïnstalleerd
- Ofwel omdat het systeem heeft geprobeerd de 'niet-revocatie' te controleren en de controleserver op internet onbereikbaar was.
Het probleem van niet-revocatie controle is gelinkt, ofwel aan uw internetverbinding, ofwel aan het feit dat uw internettoegang de crl-controle niet toelaat.Contacteer hiervoor uw netwerkbeheerder. Hij moet er voor zorgen dat
c) er geen «caching» van de crl's gebeurt
d) er geen authentificatie of een http/1.0. authentificatie op de website van certipost is.
Zie de procedure beschreven onder punt 1 (INSTALLATIE & CONFIGURATIE) en zorg ervoor dat de optie « ***Wanneer mogelijk succesvolle controle op certificaatintrekking vereisen bij verificatie van handtekeningen*** » gedesactiveerd wordt. Bijkomende details over de handtekening kan men bekomen via het tabblad 'signatures' links van het document.