Beveiliging en controle van de PDF-documenten

De documenten zijn gecertificeerd door Dexia 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 ?

- **Authenciteit** : Gaat het zeker om een origineel document afgeleverd door Dexia Bank ? De controle wordt gerealiseerd door middel van een root-certificaat. Zo is men zeker van de authenciteit 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-cerficaat te installeren op uw PC.

Op dit ogenblik functioneert de controle van de elektronische handtekening enkel met de software ADOBE READER versie 7 of hoger. Het gebruik van een lagere versie geeft een foutmelding. Deze onvereneigbaarheid ontstaat doordat het gebruikte certificaat van nieuwe generatie (2048 bits) niet verenigbaar is met de oudere versies van ADOBE READER. . Wij raden aan om een gratis upgrade uit te voeren van ADOBE READER (via de website www.adobe.be). Deze upgrade is beschikbaar voor alle PC's uitgerust met een versie Windows 2000 SP3 of hoger.
Indien u Adobe 7 niet geïnstalleerd heeft en u gebruikt Adobe 6, ontvangt u de boodschap dat de handtekening niet geldig is. U hoeft met deze boodschap geen rekening te houden !

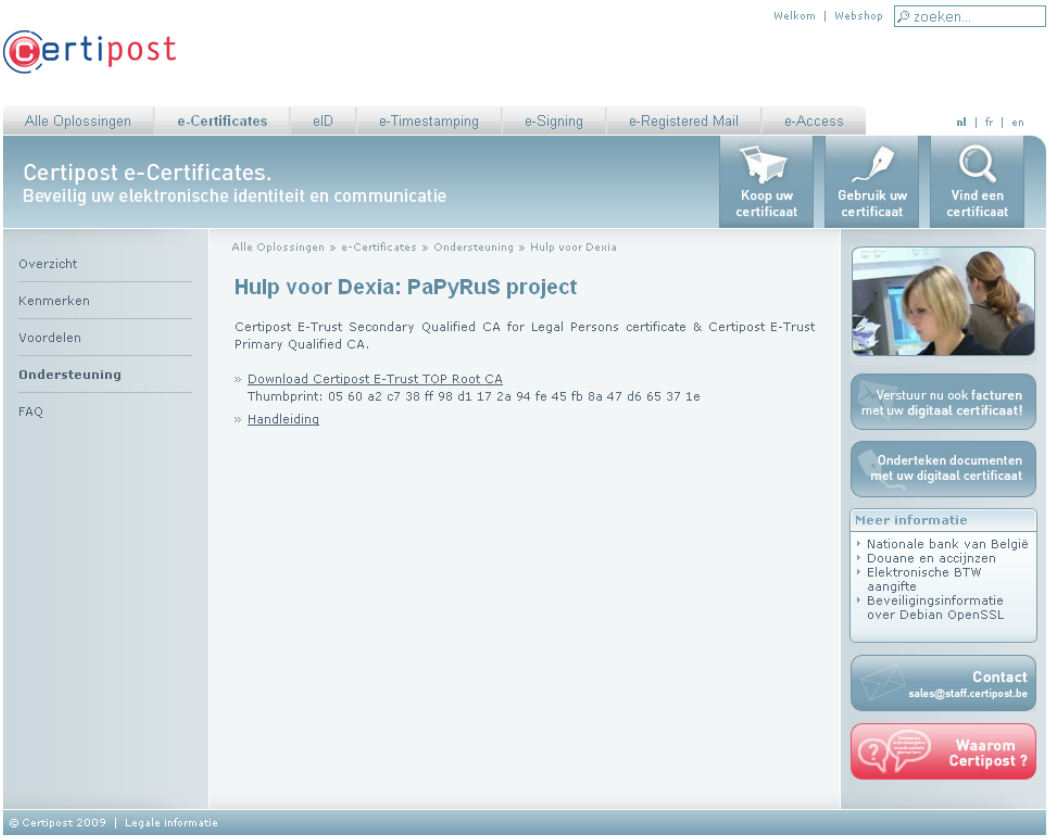
Om het certificaat te installeren kunnen er twee procedures worden gevolgd (naar keuze) => Volg de stappen van hoofdstuk 1 **of** hoofdstuk 2.

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

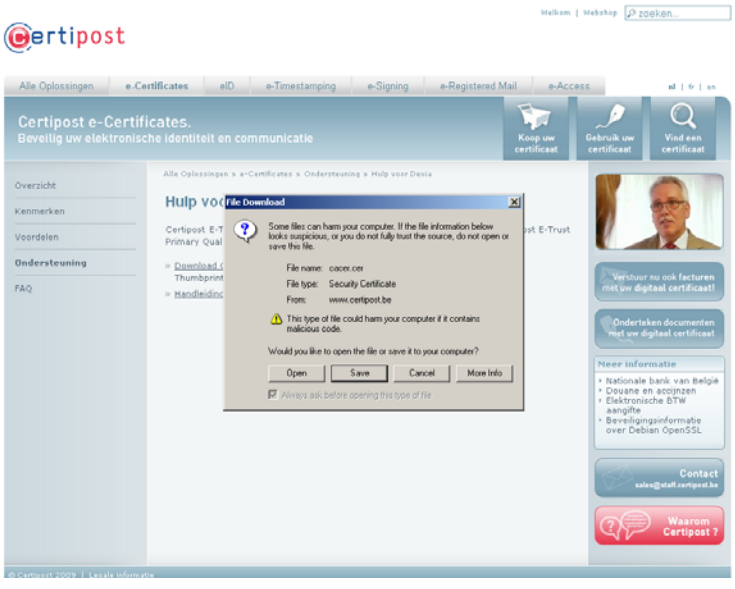
1. INSTALLATIE via WINDOWS & CONFIGURATIE VAN ADOBE READER

1.1. Installatie vanuit WINDOWS

- Het 'root-certificaat' is beschikbaar :
  - Via de internetsite gelinkt aan PAYRUS.
  - Rechtstreeks op de site van Certipost. (onafhankelijke bron)
    http://www.certipost.be/dpsolutions/nl/e-certificates-support-hulp-voor-dexia.html

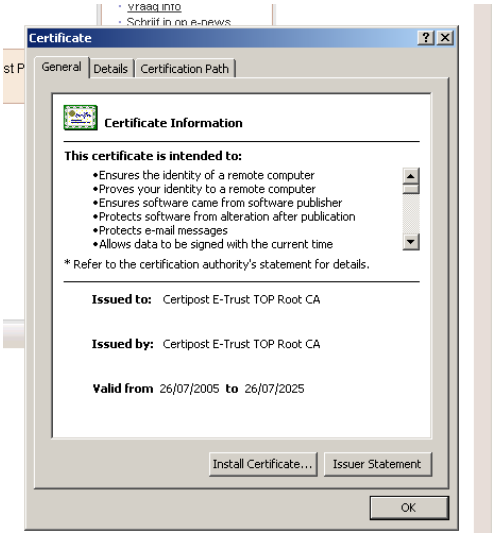


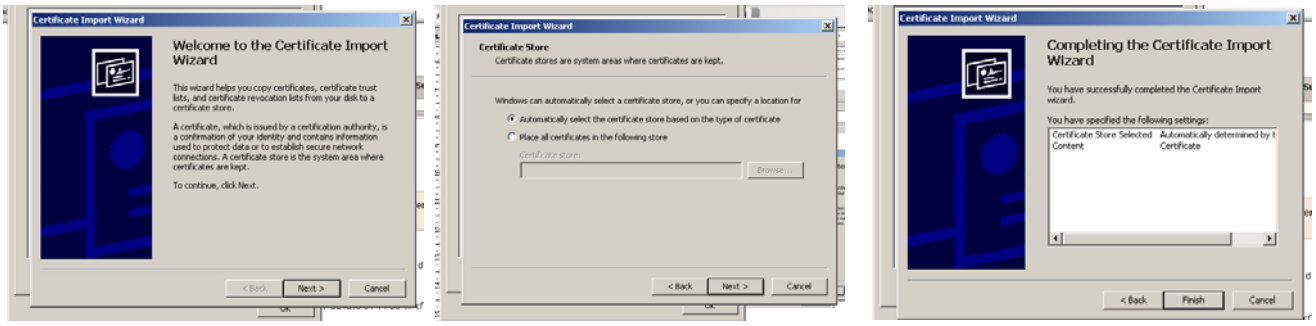
- Surf naar de opgegeven site et klik op het certificaat **« Download Certipost E-Trust TOP Root CA Thumbprint: 05 60 a2 c7 38 ff 98 d1 17 2a 94 fe 45 fb 8a 47 d6 65 37 1e »**.



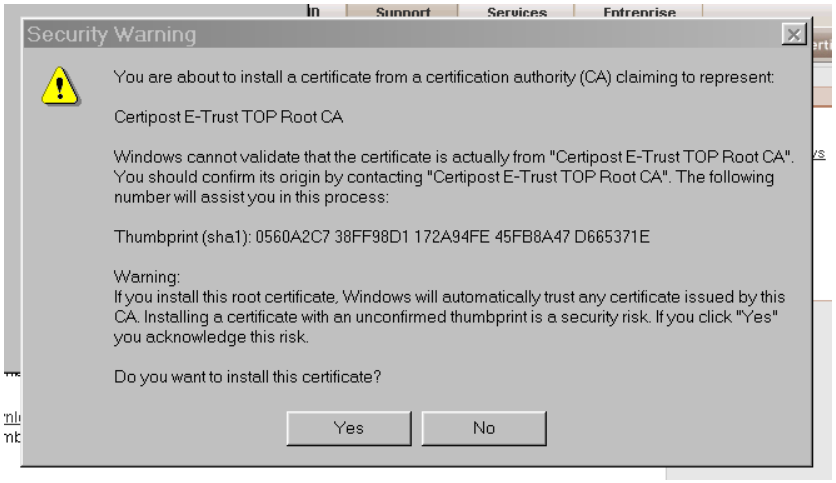
- Er verschijnt een venster vraagt of het bestand moet worden geopend (« Open ») of opgeslagen (« Save »). Kies « Open ».

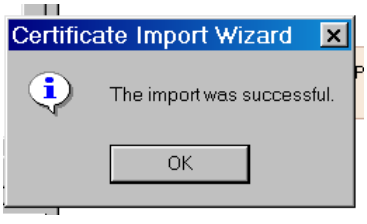
- Er verschijnt een venster dat de eigenschappen van het certificaat toont. Klik op de knop « INSTALL CERTIFICATE ».





Het volstaat om vervolgens de voorgestelde opties te bevestigen (kies twemmal 'Next' en vervolgens 'Finish')



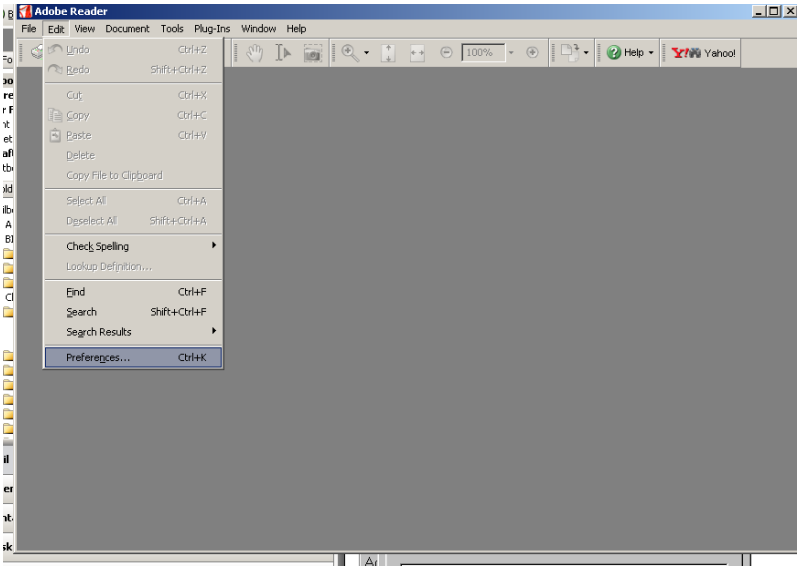


Er wordt nogmaals een bevestiging gevraagd : kies « Yes », dan « OK »

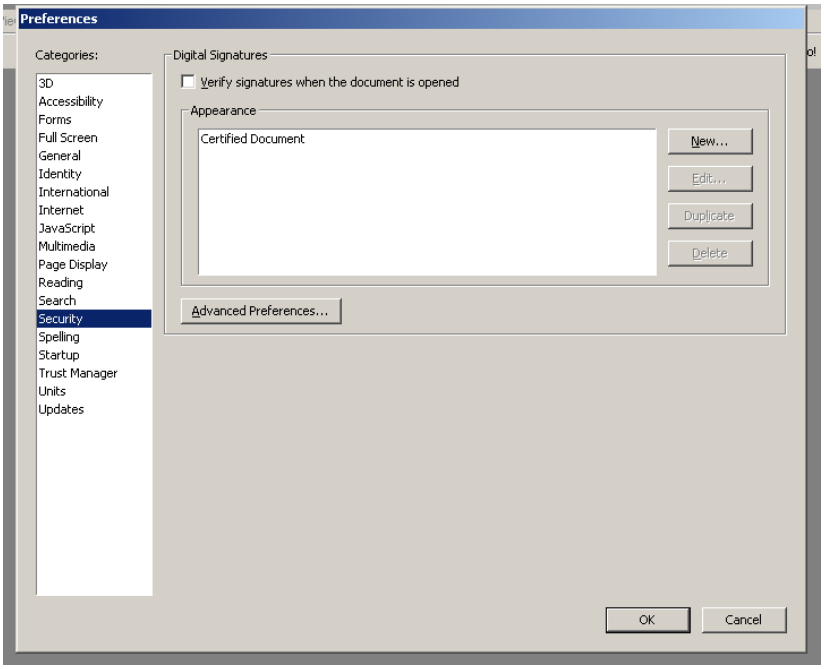
- Via deze procedure is het certificaat geïnstalleerd in de 'root-store' van Windows. Met 2e stap wordt de toepassing ADOBE toegelaten het certicaat te gebruiken.

1.2. Configuratie van de toepassing ADOBE (adobe reader 7.0).

Kies het menu EDIT / PREFERENCES => een venster wordt geopend.



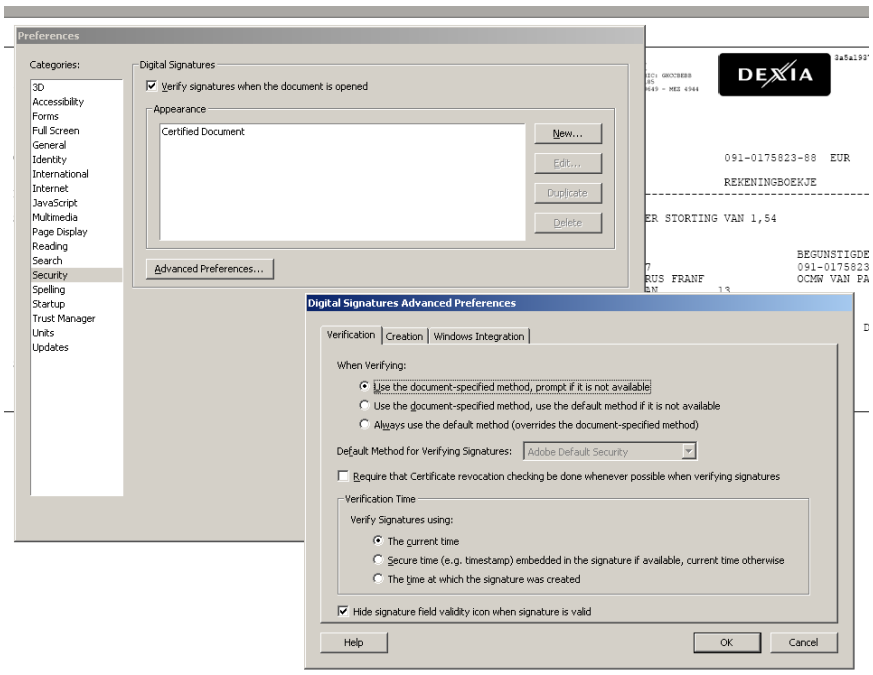
Kies het onderdeel : SECURITY/ADVANCED PREFERENCE



Het nieuwe venster bevat 3 tabbladen.

Tabblad 1 : VERIFICATION

De optie **'require that certificate revocation checking be done…"** Geeft aan of de contrôle 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 contrôle en de afhankelijkheid van internet, bent u vrij, al dan niet deze optie te activeren.



Bijkomende opmerking (enkel als de hierboven vermelde optie geactiveerd is).

De CRL controle gebeurt via het Internet : Als uw internet-toegang via een proxy gebruikt wordt, moet u ook zorgen dat die proxy correct geparametriseerd is om die CRL controle toe te laten. Contacteer hiervoor uw netwerk-beheerder. Hij moet er voor 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.

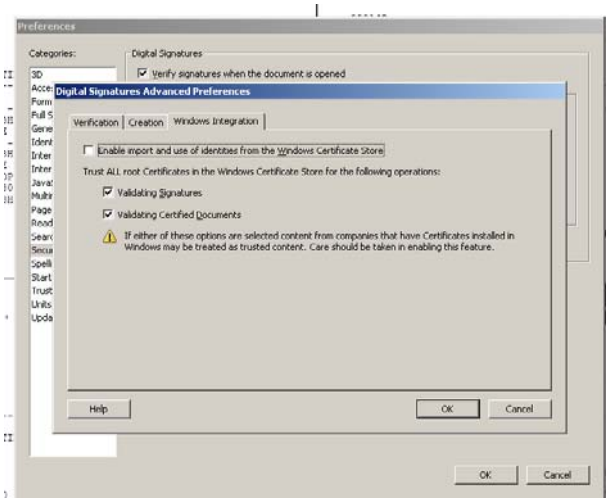
De niet-revocatie controle is nodig om te kunnen verifiëren dat het –door Dexia Bank gebruikte certificaat om het plaatsten van de digitale handtekening- niet werd gerevoceerd. Een certificaatrevocatie is –in het geval van PaPyRuS- puur theoretisch. Die certificaten zijn inderdaad op beveiligde apparatuur 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 (list van gerevoceerde certificaten)

Onglet 3 : Windows Integration : Activeer de optie '**Validating certified document**'.

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.

U kan de geopende vensters sluiten door tweemaal op OK te klikken

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 hercontroleren. Hiervoor dient men rechts te klikken op het icoontje van de handtekeningen en de optie '**Validate Signature**' kiezen.



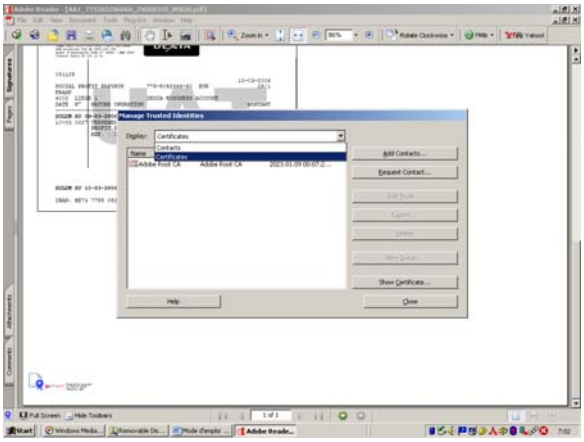
2. INSTALLATIE direct vanuit ADOBE.

Als u de onder punt 1vermelde procedure hebt gevolg, is die procedure NIET nodig.

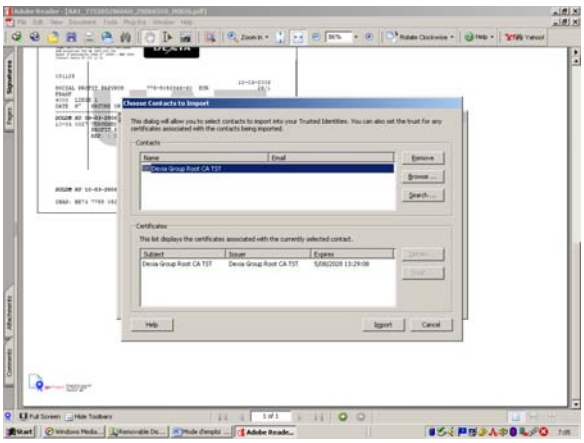
- De 'root-certificate' is beschikbaar :
  - Via de internetsite gelinkt aan PAYRUS.
  - Rechtstreeks op de site van Certipost. (onafhankelijke bron)
    http://www.certipost.be/dpsolutions/nl/e-certificates-support-hulp-voor-dexia.html

- Surf naar de opgegeven site en klik op het certificaat **« Download Certipost E-Trust TOP Root CA Thumbprint: 05 60 a2 c7 38 ff 98 d1 17 2a 94 fe 45 fb 8a 47 d6 65 37 1e »**. Er verschijnt een venster met de vraag of het bestand moet worden geopend (« Open ») of opgeslagen (« Save »). Kies « SAVE ». U moet nu de plaats aanduiden waar het certificaat wordt opgeslagen (lokaal)

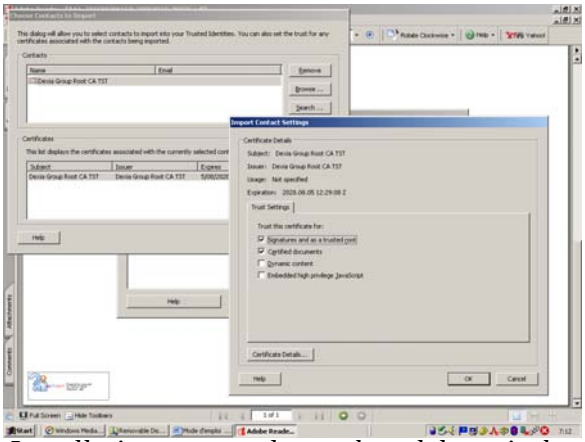
In de toepassing ADOBE, kies het Menu DOCUMENT / TRUSTED IDENTITIES => een venster wordt geopend.



Kies in 'display', het onderwerp « CERTIFICATES » en klik vervolgens op de knop 'Add Contacts..'.



Een tweede venster wordt geopend. Kies de optie 'BROWSE' en u vindt het certificaat dat het voordien heeft opgeslagen. Selecteer het certificaat en klik vervolgens op TRUST.



Het volgende venster geeft u de mogelijkheid om de karakteristieken van het gebruik van het certificaat te kiezen. Kies de opties « signature and as a trusted root » & « Certified Document ». Klik OK.

Het certificaat wordt rechtstreeks geïnstalleerd onder 'trusted identities' van Adobe.

3. **HOE EEN GEOPEND DOCUMENT CONTROLERN**

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

Is het resultaat zoals in voorbeeldafbeelding 1, dan kan u uw document als volledig geldig en integer beschouwen.

Is het resultaat zoals in voorbeeldafbeelding 2, 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 initiele 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 DexiaWeb

Is het resultaat zoals in voorbeeldafbeelding 3, dan werd bij de controle geen onregelmatigheid vastgesteld, maar is de identiteit van Dexia 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 internet-toegang de crl-controle niet toelaat.
Contacteer hiervoor uw netwerk-beheerder. 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 het punt 1 (INSTALLATIE & CONFIGURATIE) en zorg ervoor dat de optie « require that certificate revocation checking be done… » gedesactiveerd wordt.

Bijkomende details over de handtekening kan men bekomen via het tabblad 'signatures' links van het document.