GEBRUIKERSHANDLEIDING

Het handtekeningbestand (FS) aanmaken op basis van de elektronische identiteitskaart met behulp van Cryptonit.

Versie 2

Inhoudsopgave

1. Doel.

Dit document beschrijft hoe u met behulp van de software Cryptonit en OpenSSL een handtekeningbestand (FS) kan aanmaken op basis van het 'signature'-certificaat van een elektronische identiteitskaart (eID).

Een handtekeningbestand (FS) is een bestand dat, op basis van het gekwalificeerde certificaat dat bij uw kanaal voor het verzenden van gestructureerde berichten werd opgeladen, gebruikt wordt om de echtheid van een aangiftebestand (FI) te garanderen bij het verzenden van aangiftes voor de Sociale Zekerheid (ASR, Dimona, DmfA, Tijdelijke Werkloosheid, Unieke Werfmelding,…) in gestructureerde vorm via de kanalen SFTP, FTP en MQLink.

2. Vereiste aanwezigheid van de ondertekenaar.

De hierbij beschreven procedure vereist dat de eigenaar van de eID aanwezig is. Bij ieder handtekeningbestand zal de eID in de kaartlezer moeten zitten en zal de eigenaar van de eID zijn pincode moeten ingeven. Dit impliceert dat als de eigenaar van de eID niet aanwezig is, en u voor een verzending van een gestructureerd bericht een handtekeningbestand moet aanmaken, u een andere eID zal moeten gebruiken. Alvorens te verzenden zal uw lokale of co-lokale beheerder in dat geval de publieke sleutel van de andere eID moeten opladen bij de instellingen van uw kanaal op de portaalsite.

3. Wat heeft u nodig?

- een elektronische identiteitskaart
- een kaartlezer
- eID middleware
  Deze (eID Quick Install) kan u downloaden van de site
  http://eid.belgium.be/nl/
- OpenSSL
  U mag een versie naar keuze kiezen. Indien u Windows gebruikt kan u bv. gebruik maken van de versie Win32 OpenSSL v1.0.0c Light die u kan downloaden van de site
  http://www.slproweb.com/products/Win32OpenSSL.html
- Cryptonit
  U kan de versie Cryptonit-0.9.7.exe downloaden vanaf deze link
  http://sourceforge.net/projects/cryptonit/files/cryptonit/0.9.7/

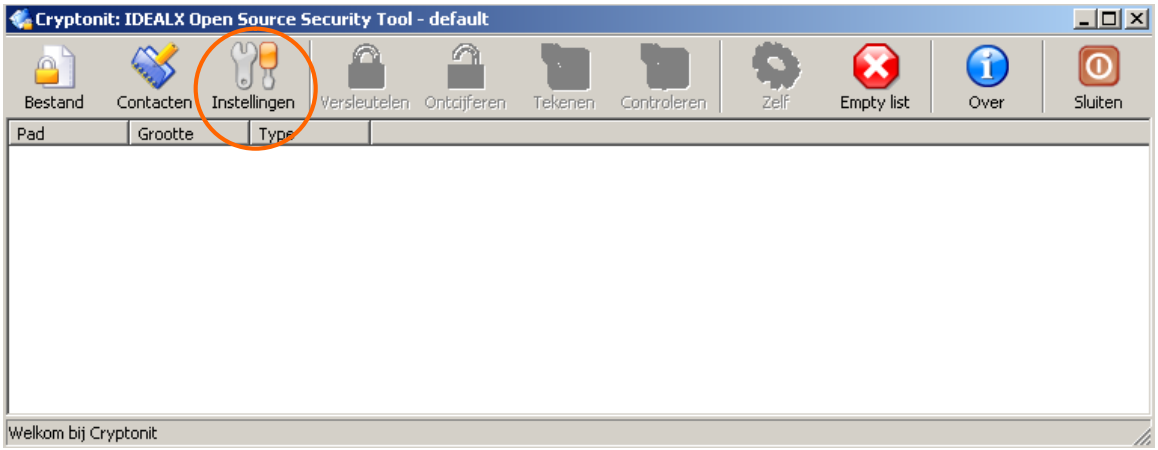
Opmerking: de in de schermafdrukken in dit document getoonde locaties voor de verschillende bestanden kunnen verschillen naar gelang het besturingssysteem dat u gebruikt.

4. Configuratie van Cryptonit.

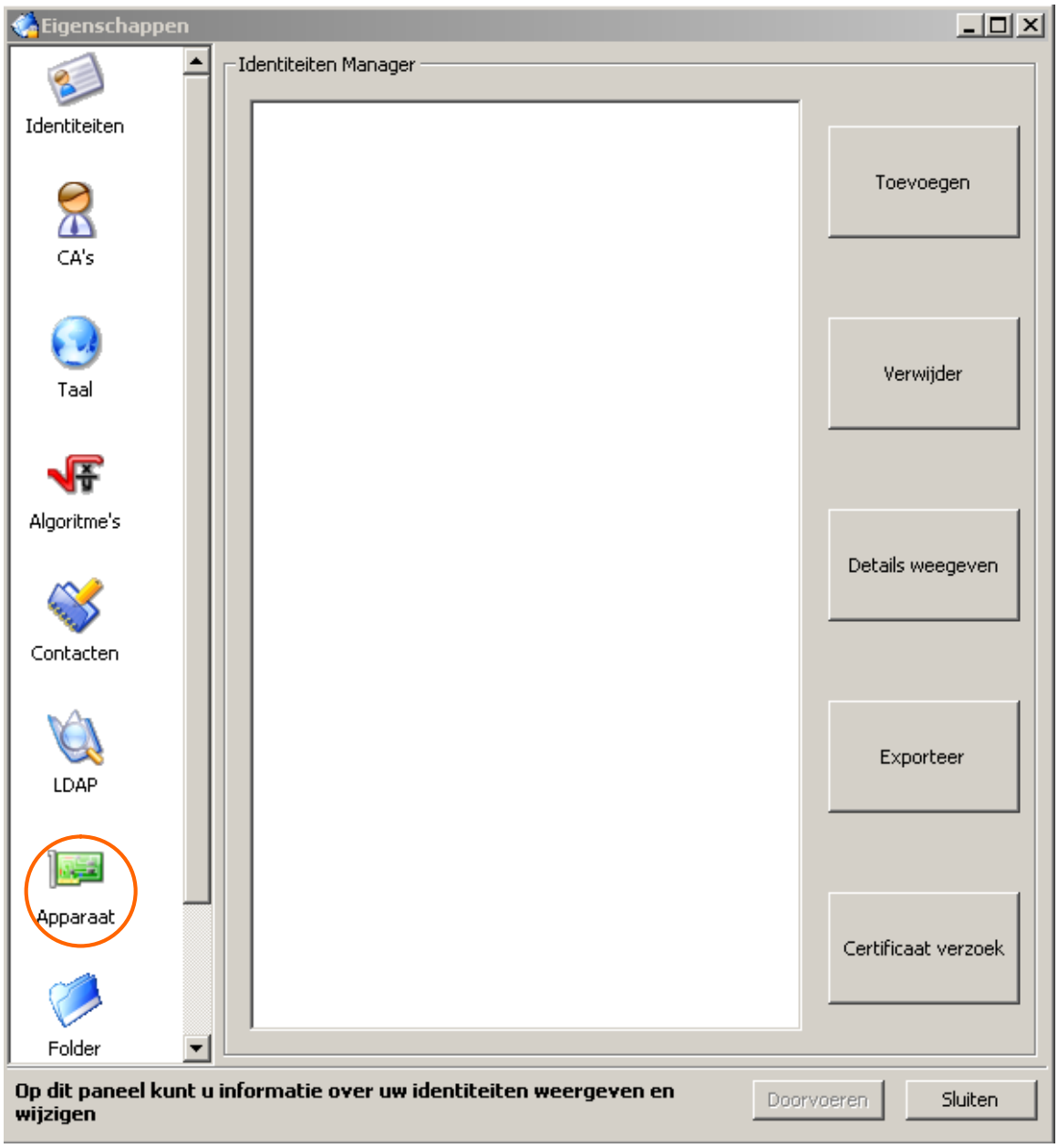
4.1. Het pkcs11-bestand toevoegen.

Start Cryptonit via Cryptonit-0.9.7.exe

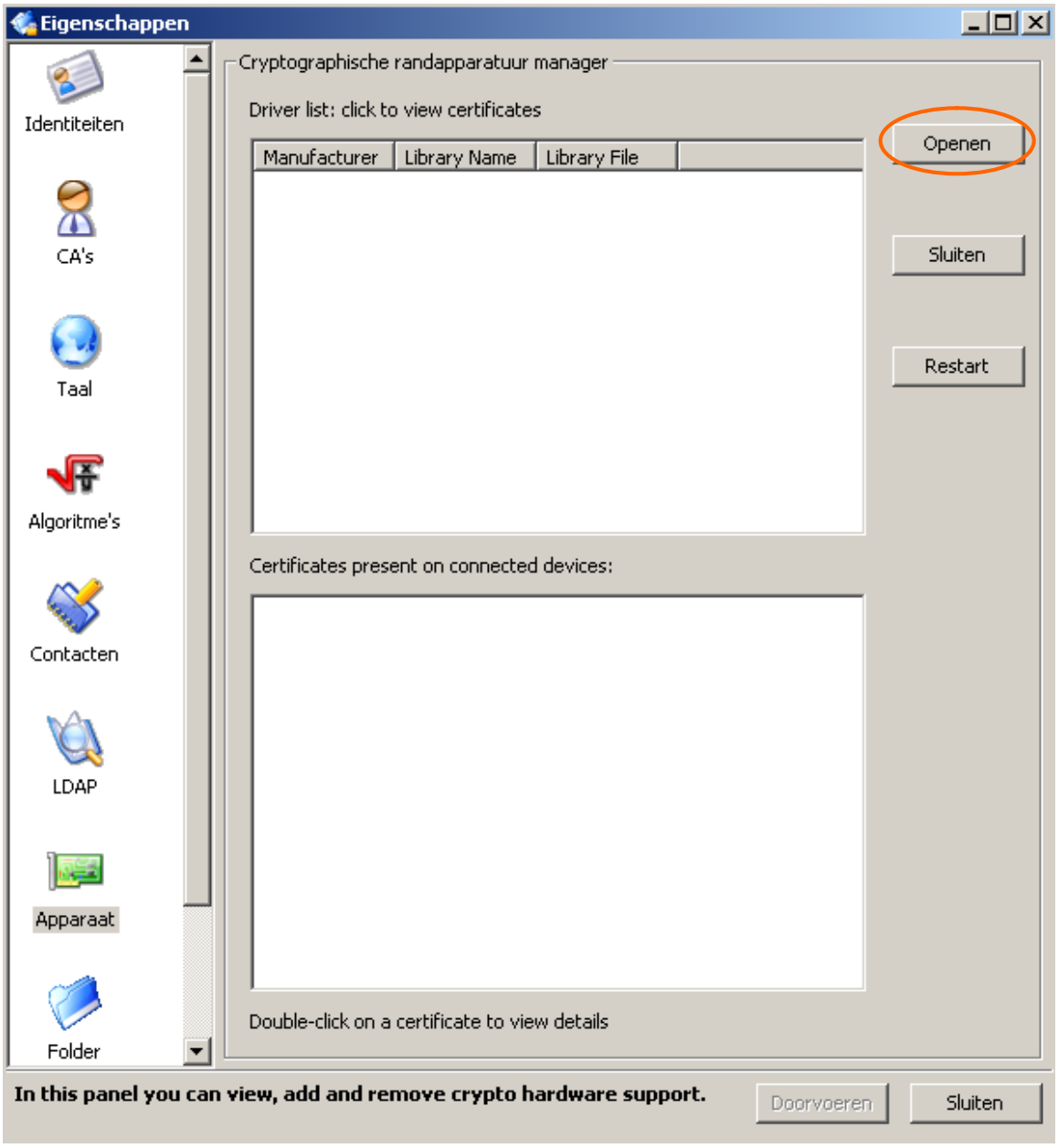
Kies ‘Instellingen/Settings’.



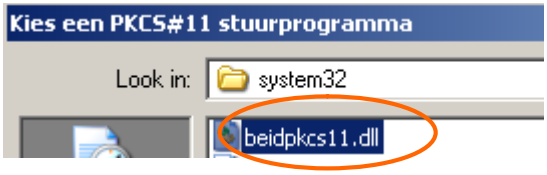
Het scherm ‘Eigenschappen/Properties’ verschijnt. Kies vervolgens het icoontje ‘Apparaat/Device’ in de linkermenu.



Klik op ‘Openen’ om het pkcs11-bestand toe te voegen.



Zoek het bestand **beidpkcs11.dll** in de map C:\WINDOWS\system32\ en klik ‘Open’.



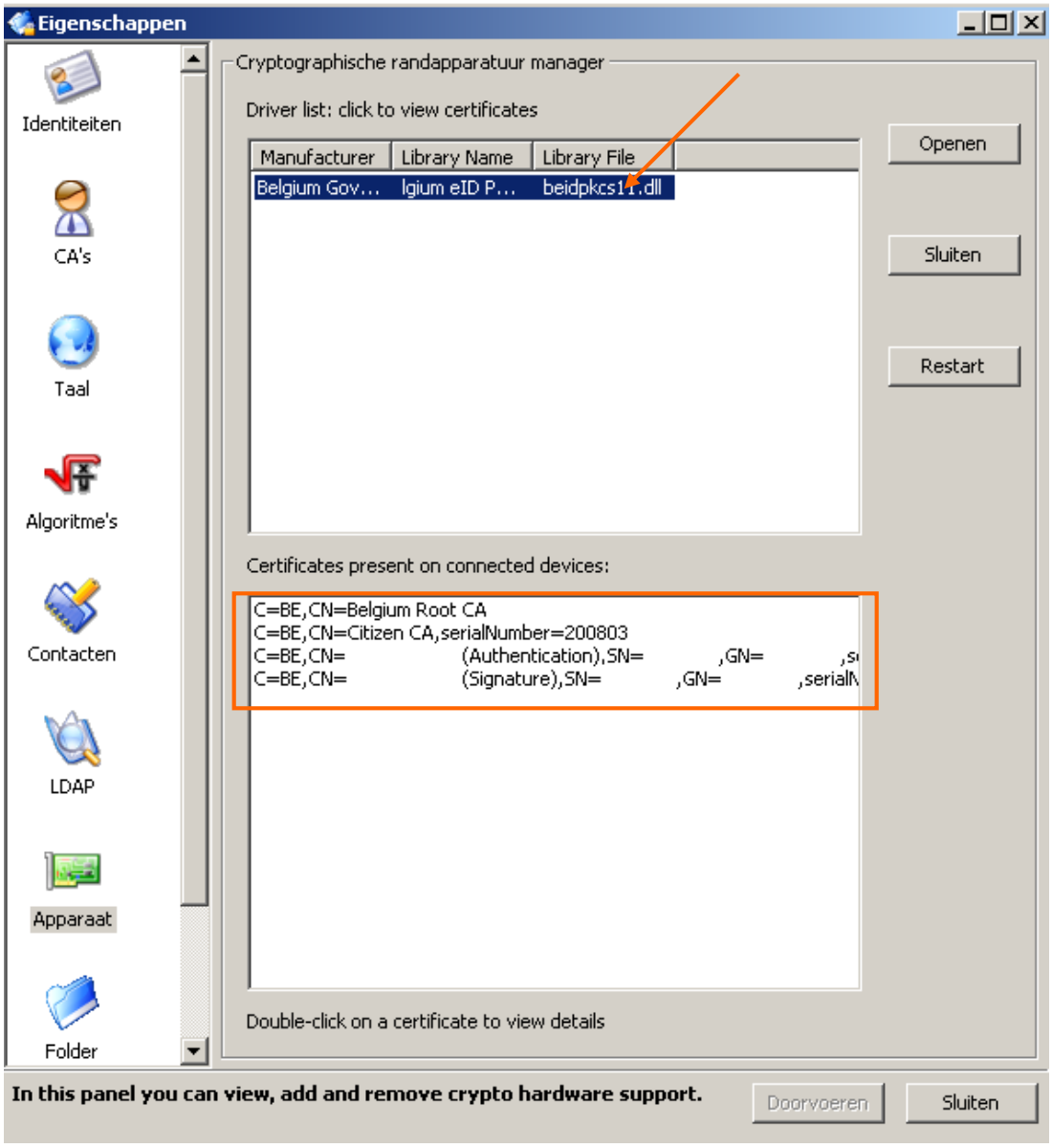
Vervolgens wordt het pkcs11-bestand toegevoegd.

4.2. Voeg de gegevens van de Certification Authority (CA) toe.

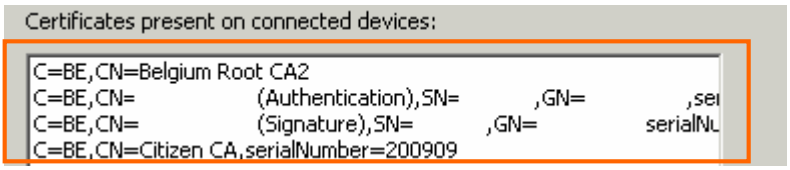
Om te weten te komen welke CA u moet toevoegen voert u volgende stappen uit:

- Steek uw eID-kaart in de kaartlezer.
- Klik op het pkcs11-bestand dat u net heeft opgeladen. Cryptonit toont nu een lijst van de geïnstalleerde certificaten en CA's.
- Afhankelijk van de identiteitskaart verschijnt dan Belgium Root CA of Belgium Root CA2. Dit onderscheid is belangrijk voor het opladen van de root CA.
- Noteer ook het serialNumber van de Citizen CA.

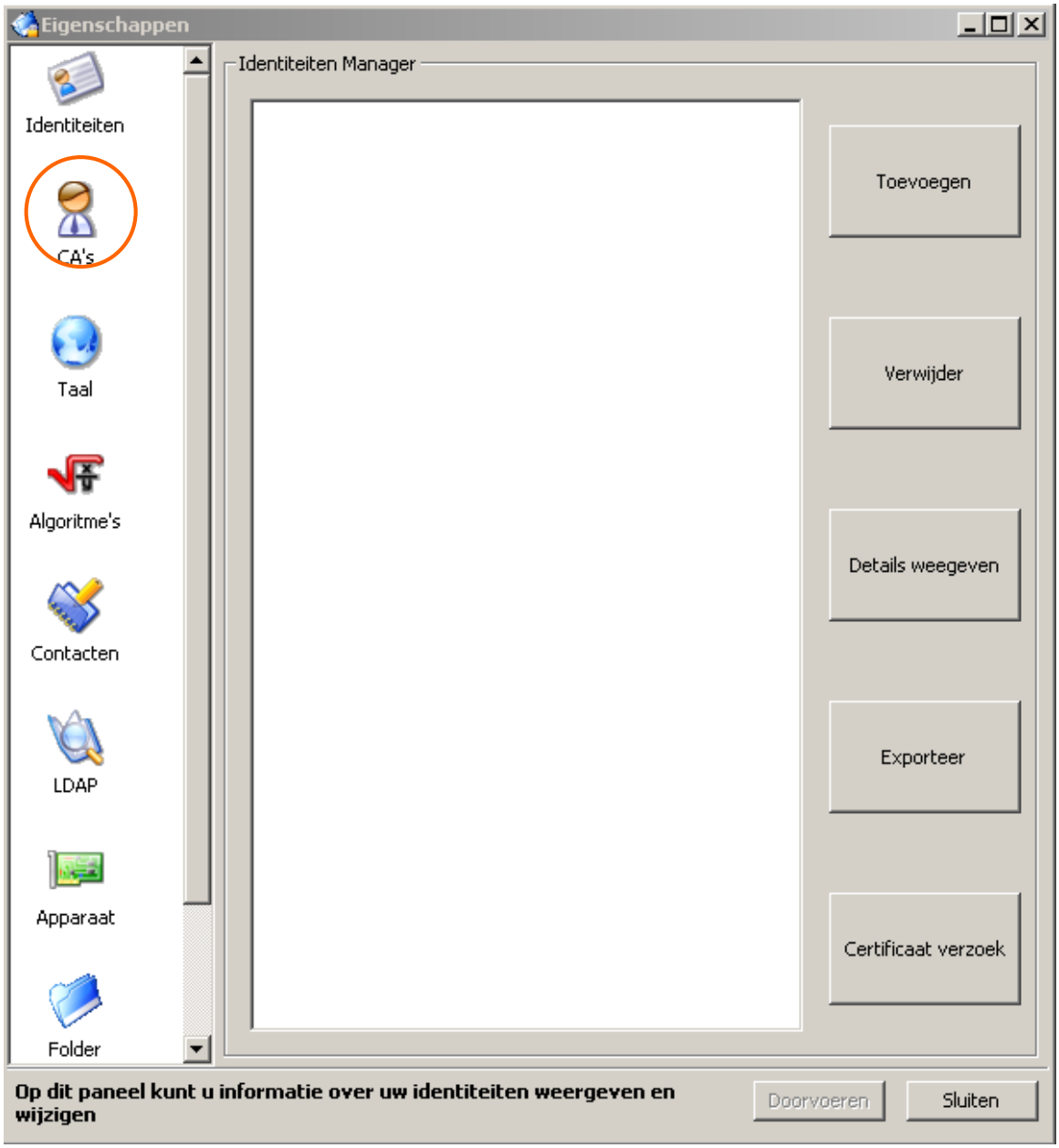
Op deze schermafdruk vindt u de Belgium Root CA en het serialNumber: 200803.



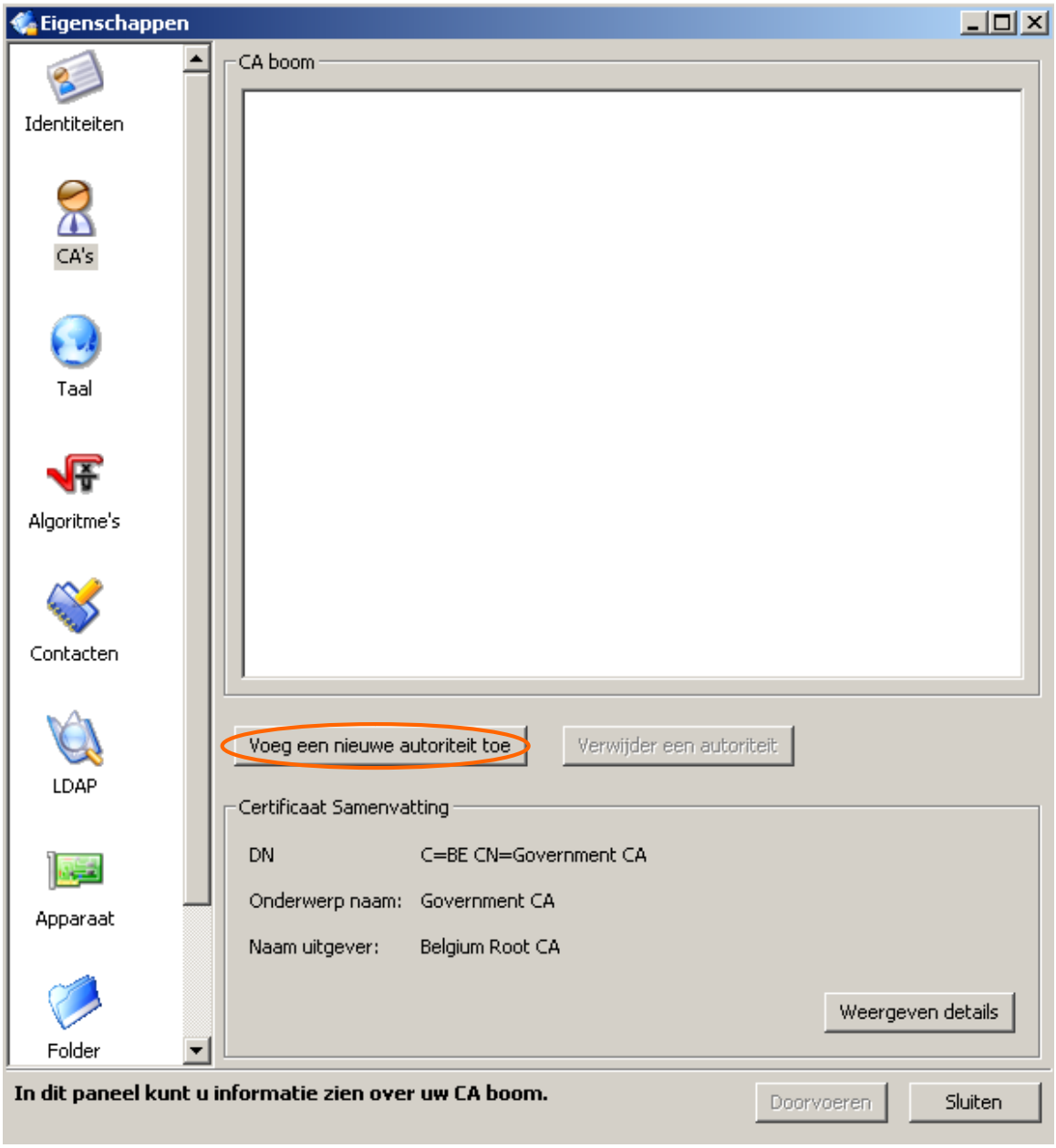
Op deze schermafdruk vindt u de Belgium Root CA2 en het serialNumber: 200909.



Kies ‘CA’s/Authorities’ in het linkermenu.



Kies ‘Voeg een nieuwe autoriteit toe/Add a new authority’.



De eerste autoriteit die moet toegevoegd worden is afhankelijk van de identiteitskaart, de Belgium Root CA of de Belgium Root CA2.

Ga naar C:\Program Files\Belgium Identity Card\eidstore\certs\

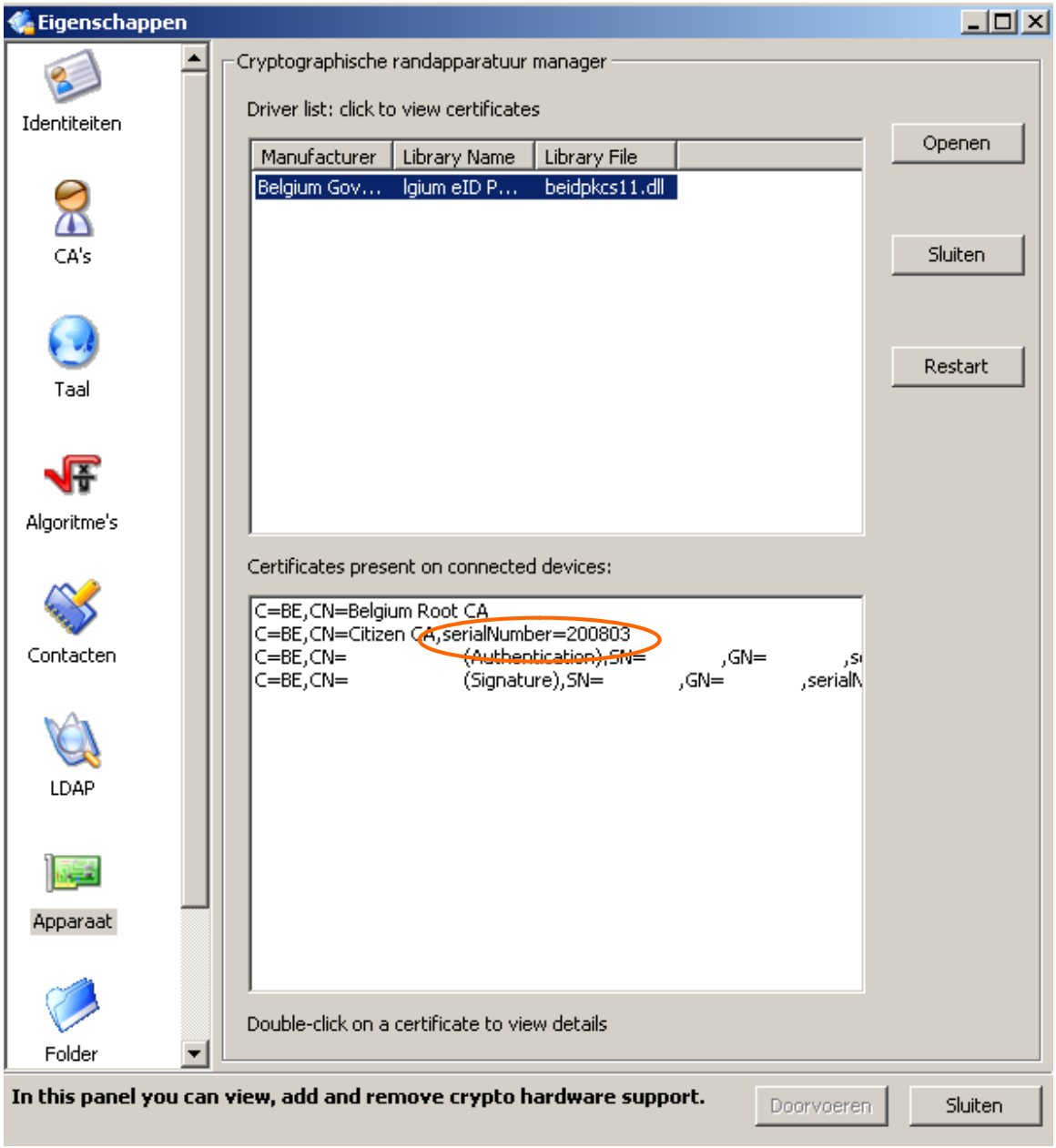
Voor Belgium Root CA:

Selecteer **beid-certbelgiumrca.der**. Klik 'Open' en de Root CA wordt toegevoegd.

Voor Belgium Root CA2:

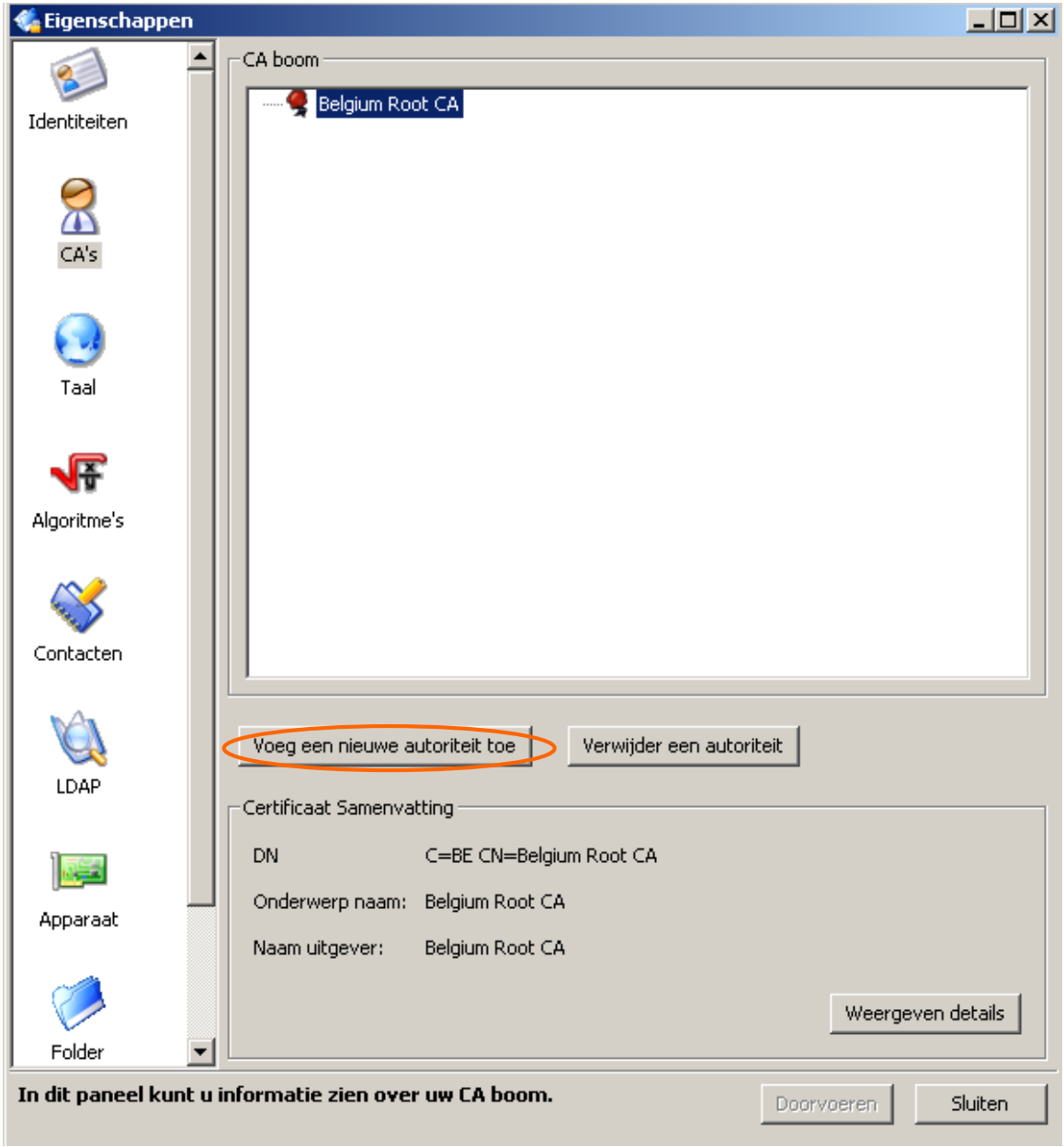
Selecteer **beid-certbelgiumrca2.der**. Klik 'Open' en de Root CA wordt toegevoegd.

De tweede autoriteit die moet toegevoegd worden is de intermediate Citizen CA. Hier is het belangrijk dat u de correcte Citizen CA kiest, namelijk diegene die uw eID heeft getekend.



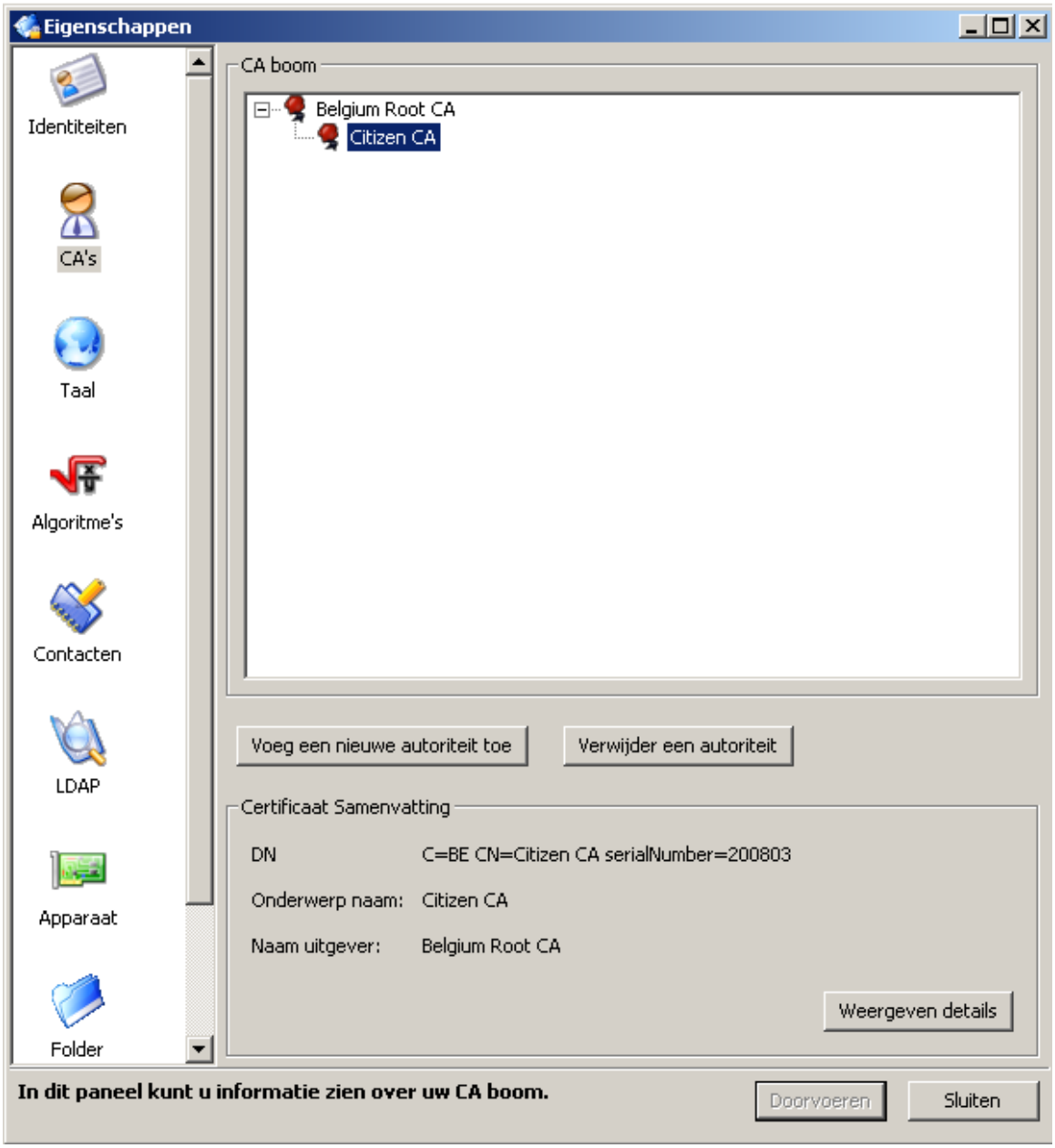
Dit kan vanuit uw browser of van de site: http://certs.eid.belgium.be/ waar u de Citizen CA met het correcte serialNumber kan downloaden.

Deze gedownloade Citizen CA in formaat .cer moet u toevoegen in Cryptonit. Kies opnieuw ‘CA’s/Authorities’ in het linkermenu en vervolgens ‘Voeg een nieuwe autoriteit toe/Add a new authority’.



Kies de .cer Citizen CA en klik ‘Open’.

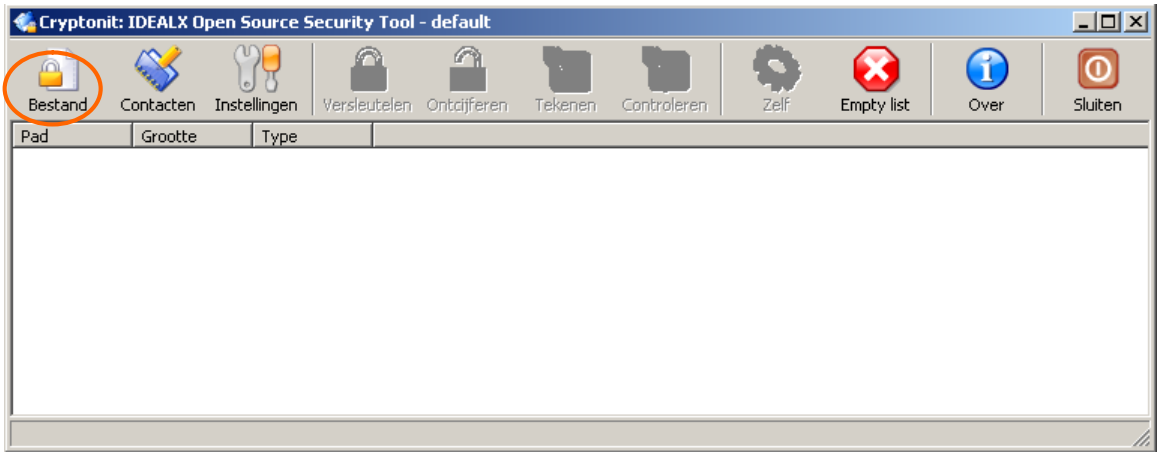
De Citizen CA is nu toegevoegd.



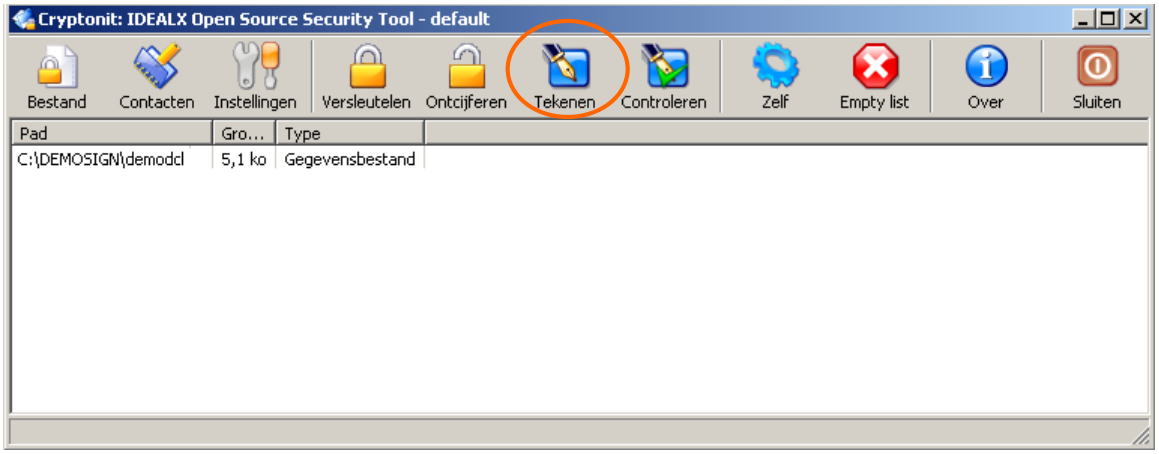
5. Uw handtekeningbestand aanmaken.

5.1. Uw aangiftebestand tekenen in DER-formaat.

Steek uw eID in uw kaartlezer.
Klik in Cryptonit op ‘Bestand/File’ en selecteer het aangiftebestand (FI) waarvoor u het handtekeningbestand (FS) wenst aan te maken.

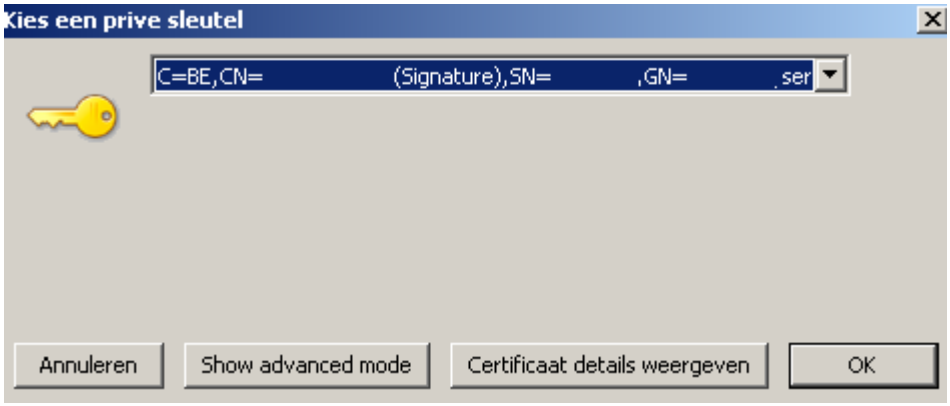


Klik vervolgens ‘Tekenen/Sign’



Kies voor ‘losgekoppeld/detached’.

Kies uw handtekening certificaat (Signature):



Vervolgens moet u 2 maal uw pincode ingeven
De eerste maal om toegang te hebben tot uw kaart.

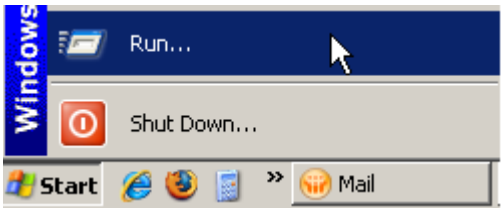
De tweede maal voor de handtekening (dit is een scherm van de eID middleware) en kan verschillend zijn naar gelang van de versie die u heeft geïnstalleerd.

Vervolgens wordt het bestand met de handtekening opgeslagen met de extensie .pkcs7 in dezelfde map als het aangiftebestand (FI).

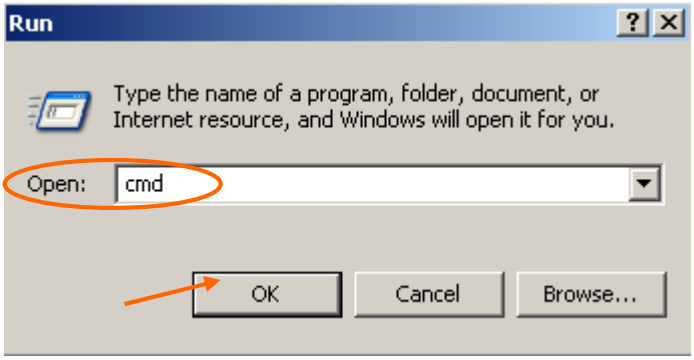
5.2. Uw handtekeningbestand omzetten naar PEM-formaat.

Met behulp van OpenSSL moet u dan nog het formaat van het bestand omzetten naar base64 encoding (DER à PEM)

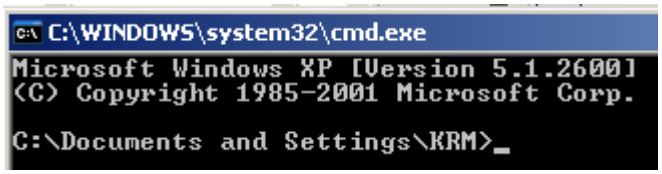
Open een dos-venster. Ga hiervoor naar **Start** en klik op **Run.**



Typ **cmd** in en klik op 'OK'.



Het dos-venster gaat open.



Vervolgens moet u naar de map gaan waar OpenSSL werd geïnstalleerd.

In dit voorbeeld werd OpenSSL in de C-map geïnstalleerd.
In dit voorbeeld kan U dit dus naar OpenSSL gaan met het commando cd C:\openssl\bin gevolgd door [ENTER]

```
> cd C:\openssl\bin
```

Geef vervolgens onderstaand commando in gevolgd door [ENTER]

>**openssl pkcs7 -in LOCATIE VAN UW MAP\NAAM VAN UW FS-BESTAND.pkcs7 -out LOCATIE VAN UW MAP\NAAM VAN UW FS-BESTAND.fs -inform der -outform pem**

Voorbeeld:
C:\OpenSSL\bin>openssl pkcs7 –in C:\DEMOSIGN\demodcl.pkcs7 -out C:\DEMOSIGN\demodcl.fs -inform der -outform pem

5.3. Manuele aanpassingen van uw FS-bestand

Voor u het bestand kan versturen moet u nog enkele manuele aanpassingen aan uw FS-bestand doen.
U opent het FS-bestand met een teksteditor zoals Textpad, Notepad of Wordpad en verwijdert de eerste (-----BEGIN PKCS7-----)en de laatste lijn (-----END PKCS7-----) inclusief de eventuele blanco lijnen ten gevolge van ENTER (carriage return).

Na deze aanpassingen kan u het bestand nog de correcte bestandsnaam geven en bewaart u uw FS-bestand d.m.v. de toetsencombinatie [CTRL]+[S].

---

6. Vrijwaringsclausule

De informatie opgenomen in dit document is louter informatief.
Hoewel al de mogelijke zorg is besteed aan de opstelling van dit document, wordt geen enkele waarborg gegeven met betrekking tot de actualiteit, accuraatheid, correctheid, volledigheid of geschiktheid hiervan.
Noch de RSZ, noch eventueel andere instantie verantwoordelijk voor de inhoud van het portaal kunnen op enigerlei wijze aansprakelijk worden gesteld voor eventuele gevolgen bij het raadplegen of het gebruik van deze gegevens.