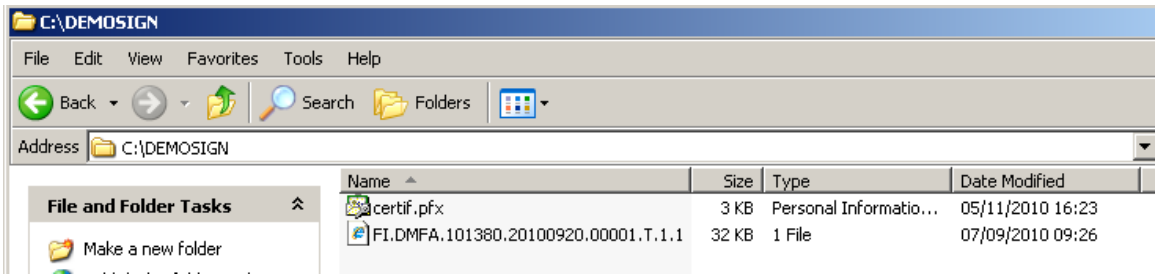
Bijlage: Een handtekeningbestand (FS) aanmaken via OPENSSL:

Opgelet:

Deze procedure is NIET geschikt voor certificaten die zich bevinden op een elektronische identiteitskaart (eID) of op een Isabelkaart. In de praktijk is deze procedure enkel bruikbaar voor certificaten van Globalsign.

Om een handtekeningbestand aan te maken met OpenSSL dient u eerst deze sofware te installeren op de PC waarop u het handtekeningbestand gaat aanmaken.
Via een zoekmachine kan heel eenvoudig gezocht worden naar OpenSSL.

Na installatie maakt u best een map aan op uw PC waarin u uw certificaat (formaat .pfx of .p12) en uw te ondertekenen FI-bestand(en) plaatst.



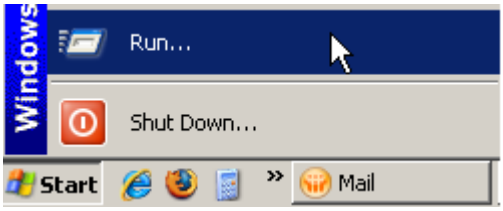
We leggen dit uit aan de hand van een voorbeeld:

- C:\DEMOSIGN : Map waarin ons FI-bestand en ons certificaat staan
- certif.pfx: naam van ons certificaat
- ww123: wachtwoord dat bij ons certificaat hoort
- ww789: wachtwoord dat we kiezen bij het aanmaken van ons .key bestand

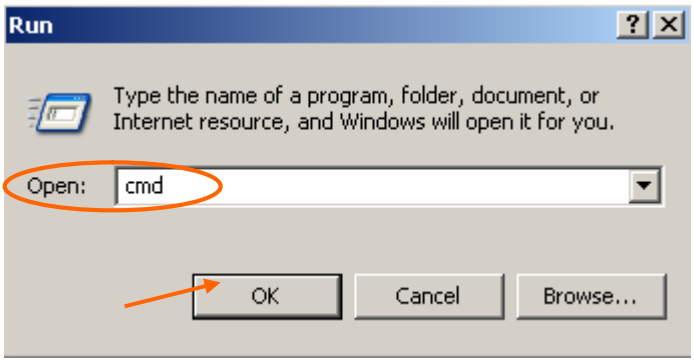
We maken een .pem-, een .key- en een FS-bestand.
We kiezen in ons voorbeeld om het .pem-bestand en het .key-bestand de naam dmfa te geven. Deze benaming is een vrije keuze. U mag ze dus gerust andere namen geven en indien u ze ook de naam dmfa zou geven mag u ze uiteraard ook voor het tekenen van bestanden voor andere toepassingen gebruiken.

Het is belangrijk om in DOS de juiste commando's en de juiste paden naar de bestanden in te typen.

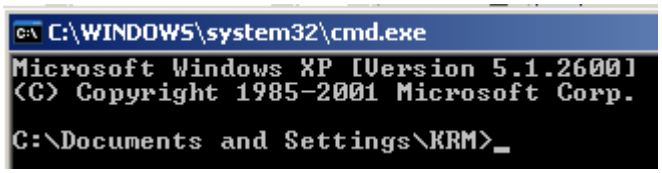
1. Open een dos-venster. Ga hiervoor naar Start en klik op **Run.**



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



En het dos-venster gaat open.



3. Vervolgens moet u naar de C-prompt gaan (dit betekent dat u een lijn heeft waar enkel '**C:\>**' staat).
Om daar te komen moet u verschillende keren het commando **cd..** gevolgd door de [ENTER]-toets ingeven.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\KRM>cd..

C:\Documents and Settings>cd..

C:\>
```

4. Open de directory OpenSSL via het commando **cd openssl** gevolgd door [ENTER]

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

5. Open de subdirectory bin via het commando **cd bin** gevolgd door [ENTER]

```
C:\OpenSSL>cd bin
```

6. Open OpenSSL via het commando **openss**l gevolgd door [ENTER]

```
C:\OpenSSL\bin>openssl
```

U krijgt nu de openSSL prompt: "OpenSSL>"

```
OpenSSL>
```

7. Nu moet u uw **.pem-bestand** aanmaken.

Na deze prompt moet u dus het commando om het .pem bestand aan te maken ingeven. Opgelet u moet hierbij gebruik maken van uw certificaat formaat .pfx of .p12 en niet van de publieke sleutel van het certificaat (.cer).

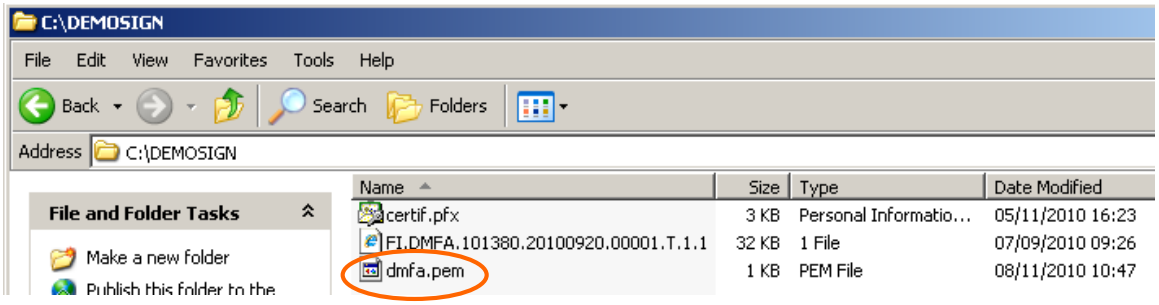
U geeft dus volgend commando met het volledige pad waar uw map met het certificaat en uw te ondertekenen FI-bestand staat in:

pkcs12 -in LOCATIE VAN UW MAP****UW CERTIFICAAT **-passin pass:**WACHTWOORD VAN UW CERTIFICAAT **-out** LOCATIE VAN UW MAP****NAAM VAN UW .PEM-BESTAND **-clcerts -nokeys** gevolgd door [ENTER]

```
OpenSSL> pkcs12 -in C:\DEMOSIGN\certif.pfx -passin pass:ww123 -out
C:\DEMOSIGN\dmfa.pem -clcerts -nokeys
```

Uw .pem-bestand wordt aangemaakt en in uw map met uw certificaat en uw aangiftebestand geplaatst.

```
OpenSSL> pkcs12 -in C:\DEMOSIGN\certif.pfx -passin pass:ww123 -out
C:\DEMOSIGN\dmfa.pem -clcerts –nokeys
MAC verified OK
```



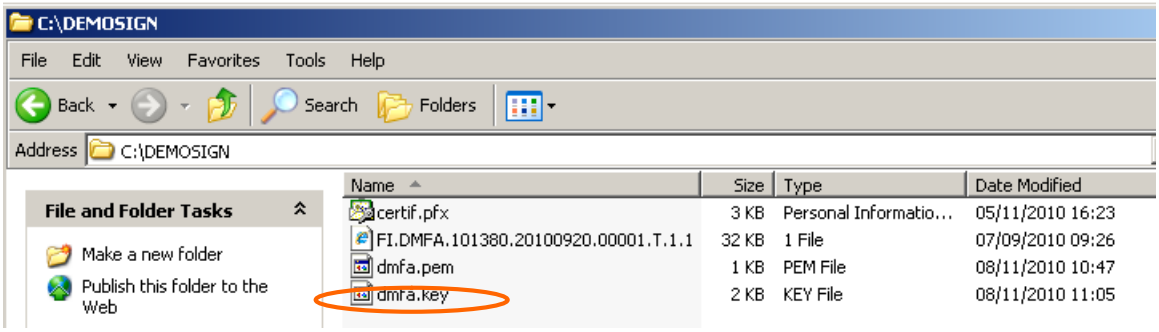
8. Nu moet u uw **.key-bestand** aanmaken

U geeft hiervoor volgend commando in na de prompt OpenSSL> :
pkcs12 -in LOCATIE VAN UW MAP****UW CERTIFICAAT **-passin pass:**WACHTWOORD VAN UW CERTIFICAAT **-passout pass:**WACHTWOORD DAT U KIEST VOOR UW .KEY **-out** LOCATIE VAN UW MAP****NAAM VAN UW .KEY-bestand gevolgd door [ENTER]

OpenSSL> **pkcs12 -in C:\DEMOSIGN\certif.pfx -passin pass:ww123 –passout pass:ww789 -out C:\DEMOSIGN\dmfa.key**

Uw .key-bestand wordt aangemaakt en in uw map met uw certificaat en uw aangiftebestand geplaatst.

OpenSSL> pkcs12 -in C:\DEMOSIGN\certif.pfx -passin pass:ww123 –passout pass:ww789 -out C:\DEMOSIGN\dmfa.key
MAC verified OK



Telkens u een FI-bestand wil doorsturen dient u op basis van het FI-bestand in combinatie met het .pem en het .key bestand een FS-bestand aan te maken.

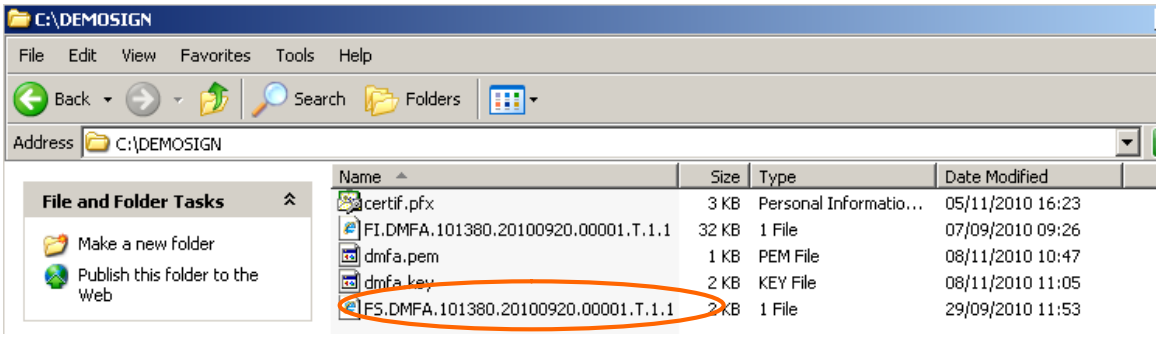
De aangemaakte .pem- en .key-bestanden kan u gebruiken zolang uw certificaat geldig is (zie Expiration Date van uw certificaat). Eens uw certificaat vervallen is moet u een nieuw certificaat opladen bij uw kanaal en moet u met uw nieuwe certificaat opnieuw de .pem- en .key-bestanden aanmaken.

9. Nu moet u uw **FS-bestand** aanmaken.

Dit FS-bestand kan u aanmaken door volgend commando in te geven na de prompt OpenSSL> :
smime -sign -in LOCATIE VAN UW MAP****NAAM VAN UW FI-BESTAND **-signer** LOCATIE VAN UW MAP****NAAM VAN UW .PEM-bestand **-inkey** LOCATIE VAN UW MAP****NAAM VAN UW .KEY-BESTAND **-passin pass:** WACHTWOORD DAT U IN STAP 8 GEKOZEN HEEFT VOOR UW .KEY **-outform PEM -out** LOCATIE VAN UW MAP****NAAM VAN UW FS-BESTAND gevolgd door [ENTER]

OpenSSL> **smime -sign -in C:\DEMOSIGN\FI.DMFA.123456.20100920.00001.T.1.1 -signer C:\DEMOSIGN\dmfa.pem -inkey C:\DEMOSIGN\dmfa.key -passin pass:ww789 -outform PEM -out C:\DEMOSIGN\FS.DMFA.123456.20100920.00001.T.1.1 -md sha256**

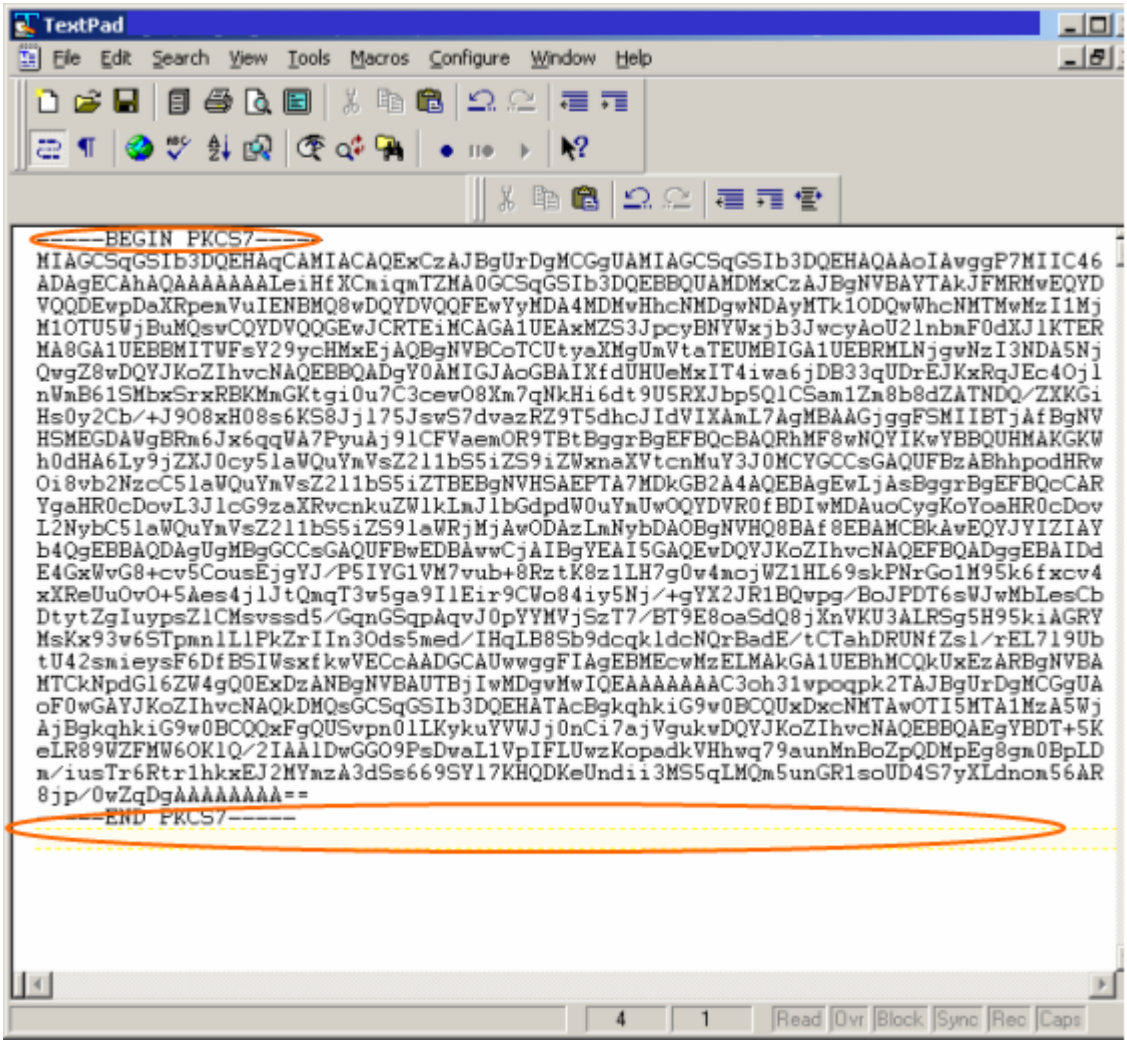
Uw FS-bestand wordt aangemaakt en in uw map met uw certificaat en uw aangiftebestand geplaatst.



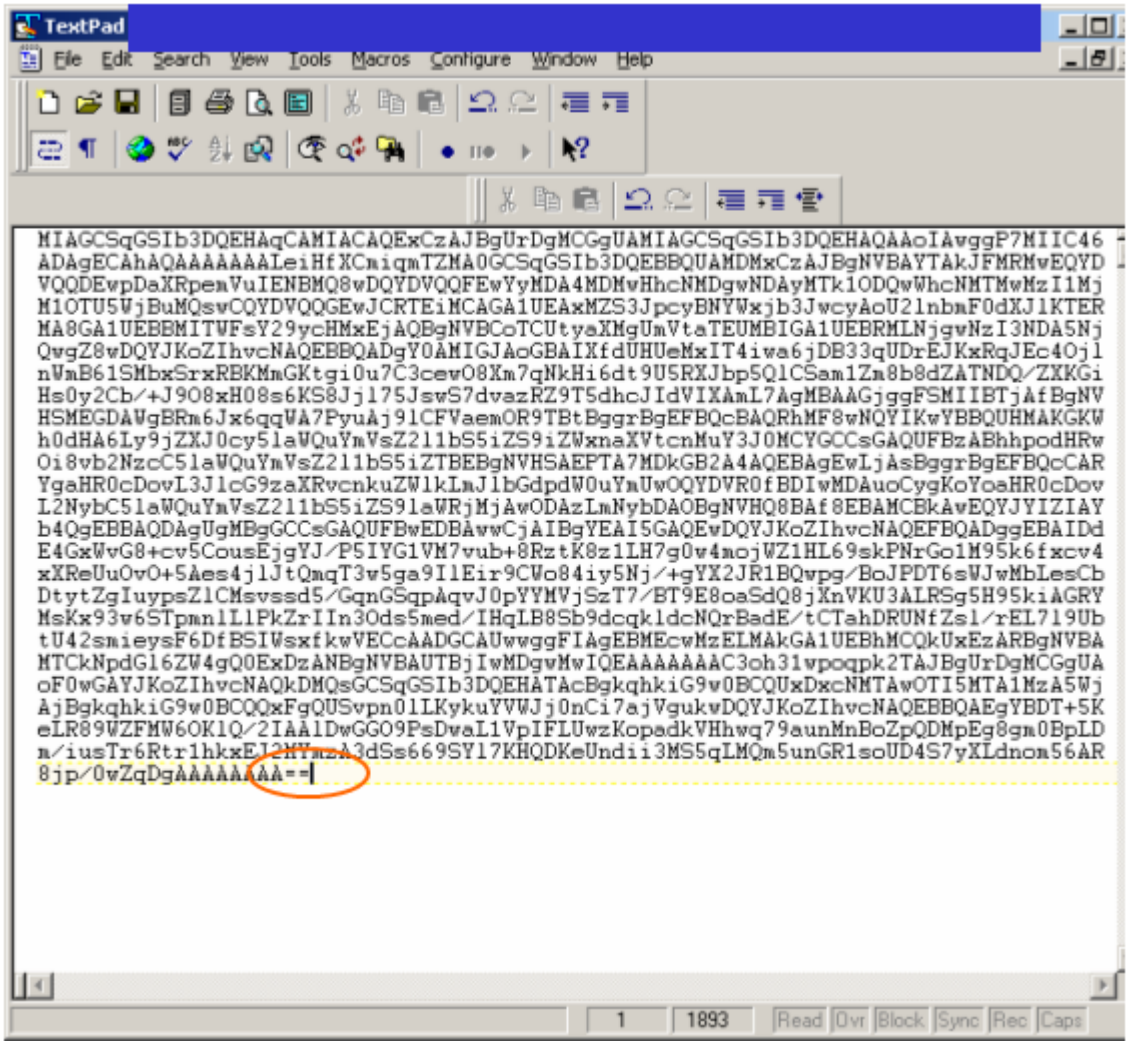
Let op: zodra u uw FS-bestand heeft aangemaakt mag u het FI-bestand niet meer wijzigen. Indien u het FI-bestand toch aanpast zal u een nieuw FS-bestand moeten aanmaken.

10. Manuele aanpassingen aan 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).



Het resultaat van uw FS-bestand wordt m.a.w:



Na deze aanpassingen bewaart u d.m.v. de toetsencombinatie [CTRL]+[S] het FS-bestand.