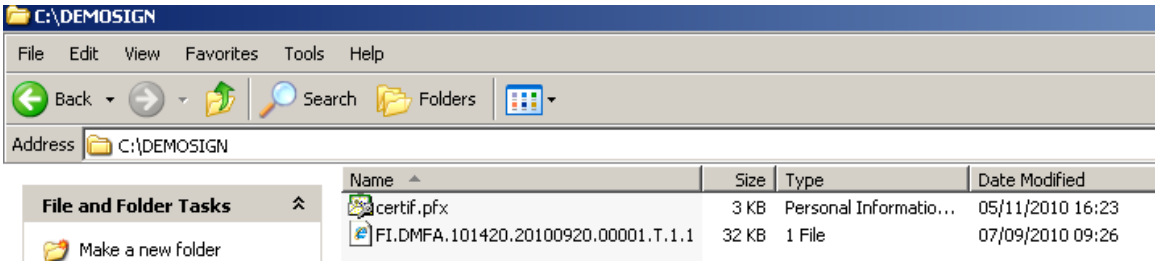
Annexe: Générer un fichier de signature avec OpenSSL :

Attention :

Cette procédure ne convient PAS aux certificats qui se trouvent sur une carte d'identité électronique (eID) ou une carte Isabel. Dans la pratique, cette procédure ne peut être utilisée que pour des certificats émis par Globalsign.

Pour créer un fichier de signature avec OpenSSL, il faut d'abord installer ce software sur le PC sur lequel vous allez créer le fichier de signature.
Via un moteur de recherche, vous pouvez rechercher très simplement OpenSSL.

Après l'installation, le mieux est que vous fabriquiez un répertoire sur votre PC dans lequel vous installerez votre certificat (format .pfx place ou .p12) et votre fichier de déclaration (FI).



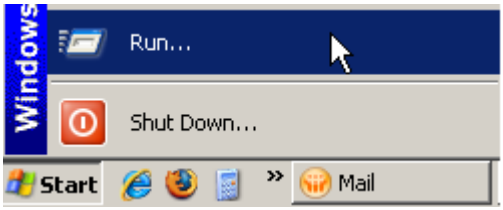
Nous expliquons ceci à l'aide d'un exemple :

- C:\DEMOSIGN : Le répertoire dans lequel se trouve le fichier de déclaration et le certificat
- certif.pfx: Nom de votre certificat
- ww123 : mot de passe du certificat
- ww789 : mot de passe que nous choisissons lors de la création de la clé

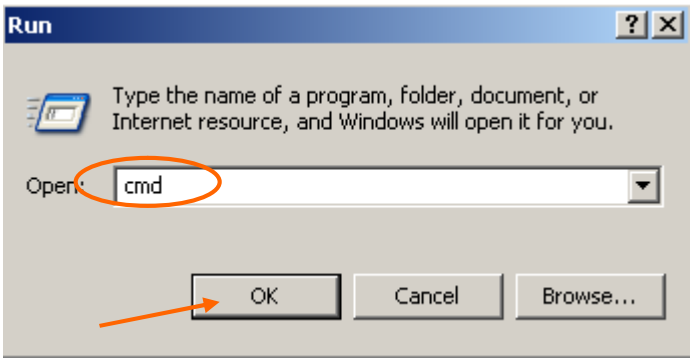
Nous allons créer un fichier .pem, un fichier .key et un fichier de signature (FS).
Nous choisissons dans notre exemple de donner le nom dmfa, au fichier .pem et au fichier .key. Cette dénomination est un libre choix. Vous pouvez choisir le nom vous-même et, même si vous choisissez le nom dmfa, vous pouvez l'utiliser pour signer les fichiers pour les autres applications.

Il est important de taper dans DOS les commandes correctes et les bons liens vers les répertoires.

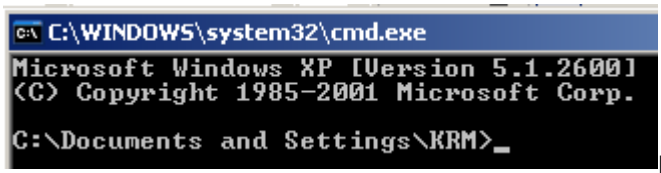
1. Ouvrez une fenêtre dos. Allez sur Start et cliquez sur **Run**



2.
3. Tapez **cmd** et cliquez sur ok



La fenêtre dos s'ouvre



µ

4. Ensuite, vous devez aller vers C-prompt (c-à-d une ligne ou vous n'avez que '**C:\>**') Pour y arriver, vous devez taper plusieurs fois **cd..** suivi de la touche [ENTER]

```
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:\>
```

5. Ouvrez le répertoire OpenSSL via la commande **cd openssl** puis cliquez sur [ENTER]

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

5. Ouvrez le sous-répertoire bin via la commande **cd bin** puis cliquez sur [ENTER]

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

6. Ouvrez OpenSSL via la commande **openss**l puis cliquez sur [ENTER]

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

Vous obtenez maintenant :

```
OpenSSL>
```

7. Vous pouvez maintenant créer **le fichier .pem**

Après ce prompt, vous devez introduire la commande pour créer le fichier .pem. Attention, vous devez, ici, utiliser votre certificat format .pfx ou .p12 et non pas la clé publique du certificat (.cer).

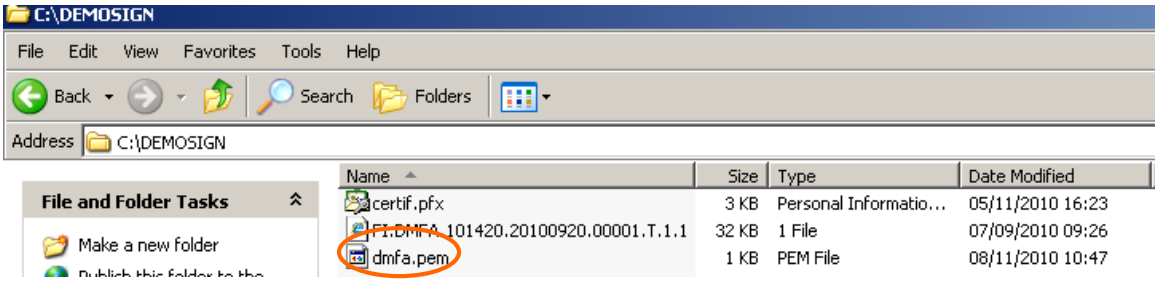
Vous introduisez la commande suivante avec le chemin complet du répertoire où se trouve le certificat et le fichier FI à signer :

pkcs12 -in Localisation de votre répertoire****votre certificat **-passin pass:** Mot de passe de votre certificat **-out** Localisation de votre répertoire****Nom de votre fichier.PEM-**clcerts -nokeys** puis cliquez sur [ENTER]

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

Votre fichier.pem est créé et placé dans le répertoire où votre certificat et votre fichier de déclaration sont placés.

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



8. Vous pouvez maintenant créer votre **fichier .key**

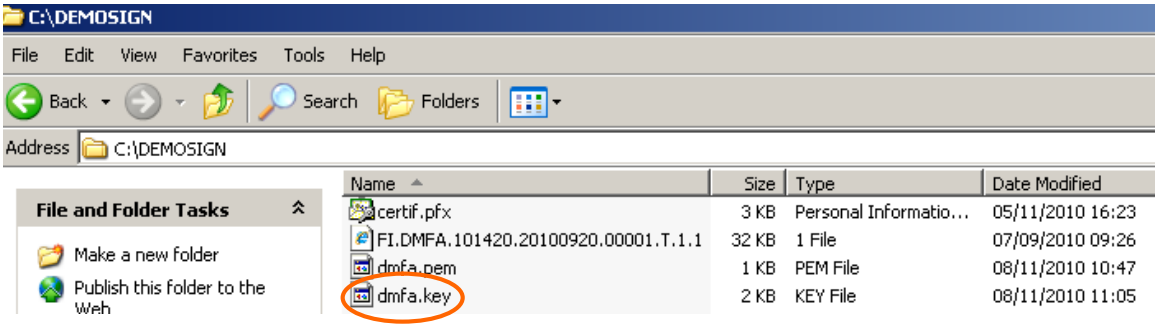
Vous introduisez la commande suivante dans le prompt OpenSSL :

pkcs12 -in Localisation de votre répertoire **** votre certificat **-passin pass:** Mot de passe de votre certificat **-passout pass:** mot de passe que vous choisissez pour votre .KEY **-out** Localisation de votre répertoire **** Nom de votre fichier.KEY puis cliquez sur [ENTER]

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

Votre fichier.key est créé et placé dans le répertoire où votre certificat, votre fichier de déclaration et votre fichier .pem sont placés.

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



Chaque fois que vous voulez envoyer un fichier FI, vous devez créer sur base du fichier FI avec les fichiers .pem et .key un fichier FS.

Vous pouvez utiliser les fichiers .pem et .key pendant toute la validité du certificat (voir Expiration Date de votre certificat). Une fois que votre certificat est périmé, vous devez charger un nouveau certificat pour le canal et vous devez créer des nouveaux fichiers .pem et .key.

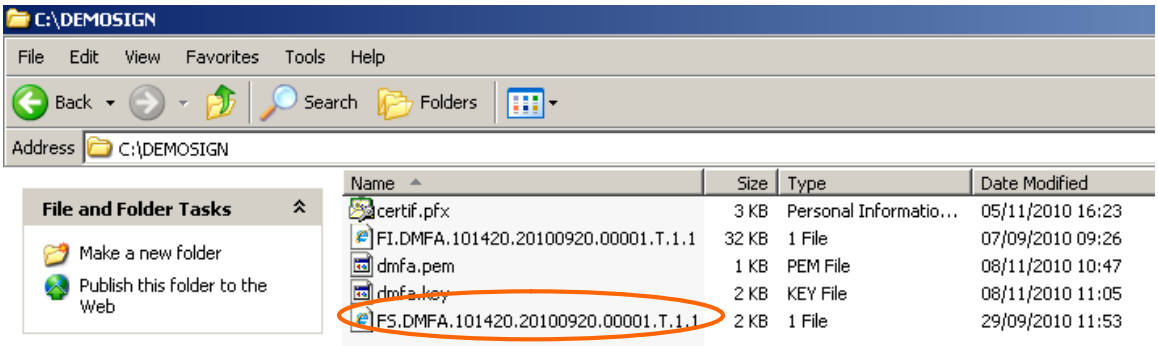
9. Vous pouvez maintenant créer votre **fichier de signature**

Le fichier FS peut être créé en introduisant les commandes suivantes dans le prompt OpenSSL :

smime -sign -in Localisation de votre répertoire****Nom du fichier FI **-signer** Localisation de votre répertoire****Nom de votre fichier .PEM **-inkey** Localisation de votre répertoire****Nom de votre fichier.KEY **-passin pass:** Mot de passe que vous avez choisi pour le .KEY **-outform PEM -out** Localisation de votre répertoire****Nom du fichier FS puis cliquez sur [ENTER]

OpenSSL> **smime -sign -in C:\DEMOSIGN\FI.DMFA.123456.20120213.00001.T.1.1 -signer C:\DEMOSIGN\dmfa.pem -inkey C:\DEMOSIGN\dmfa.key -passin pass:ww789 -outform PEM -out C:\DEMOSIGN\FS.DMFA.123456.20120213.00001.T.1.1 -md sha256**

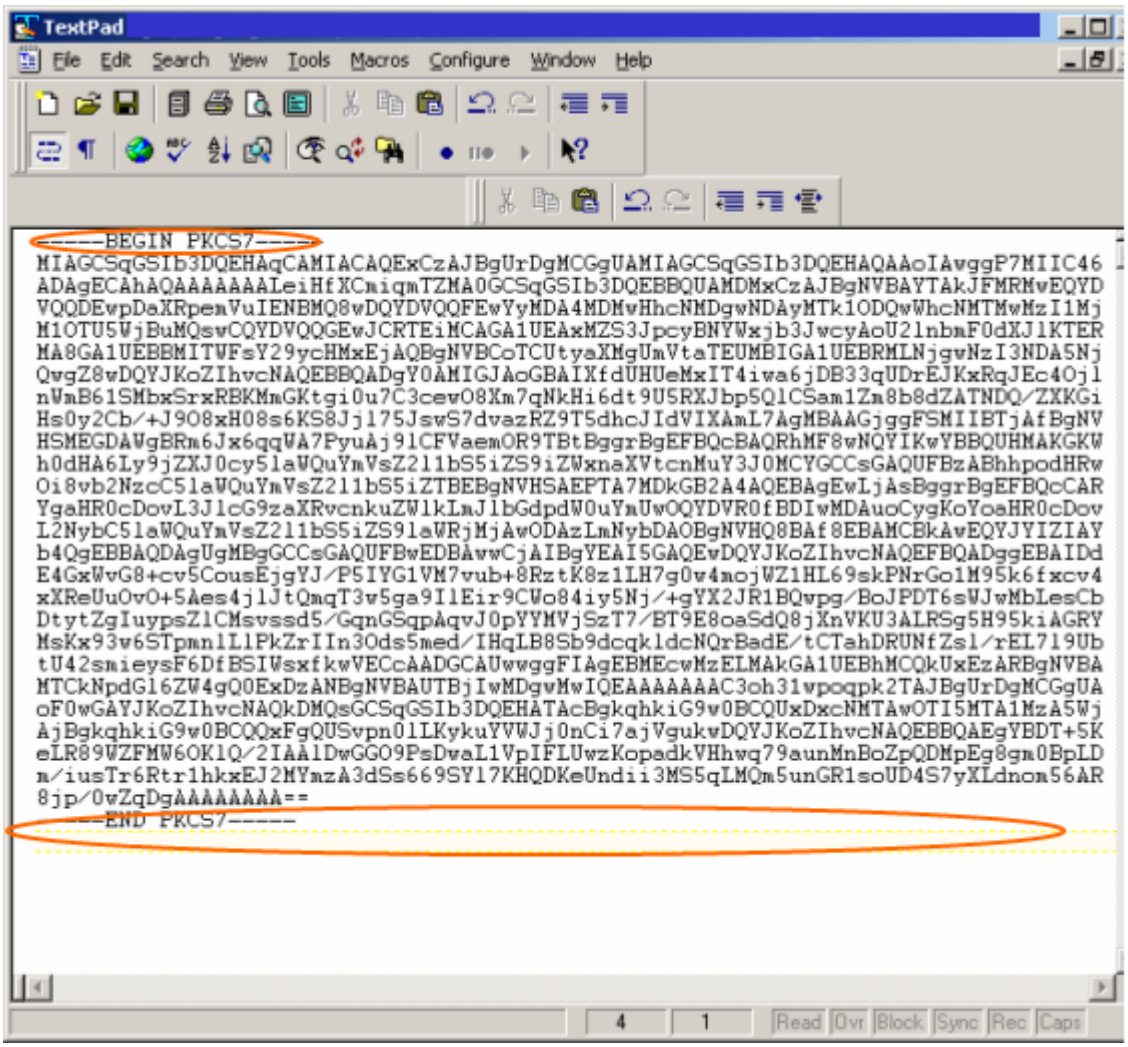
Votre fichier FS est créé dans le répertoire avec votre certificat et votre fichier de déclaration.



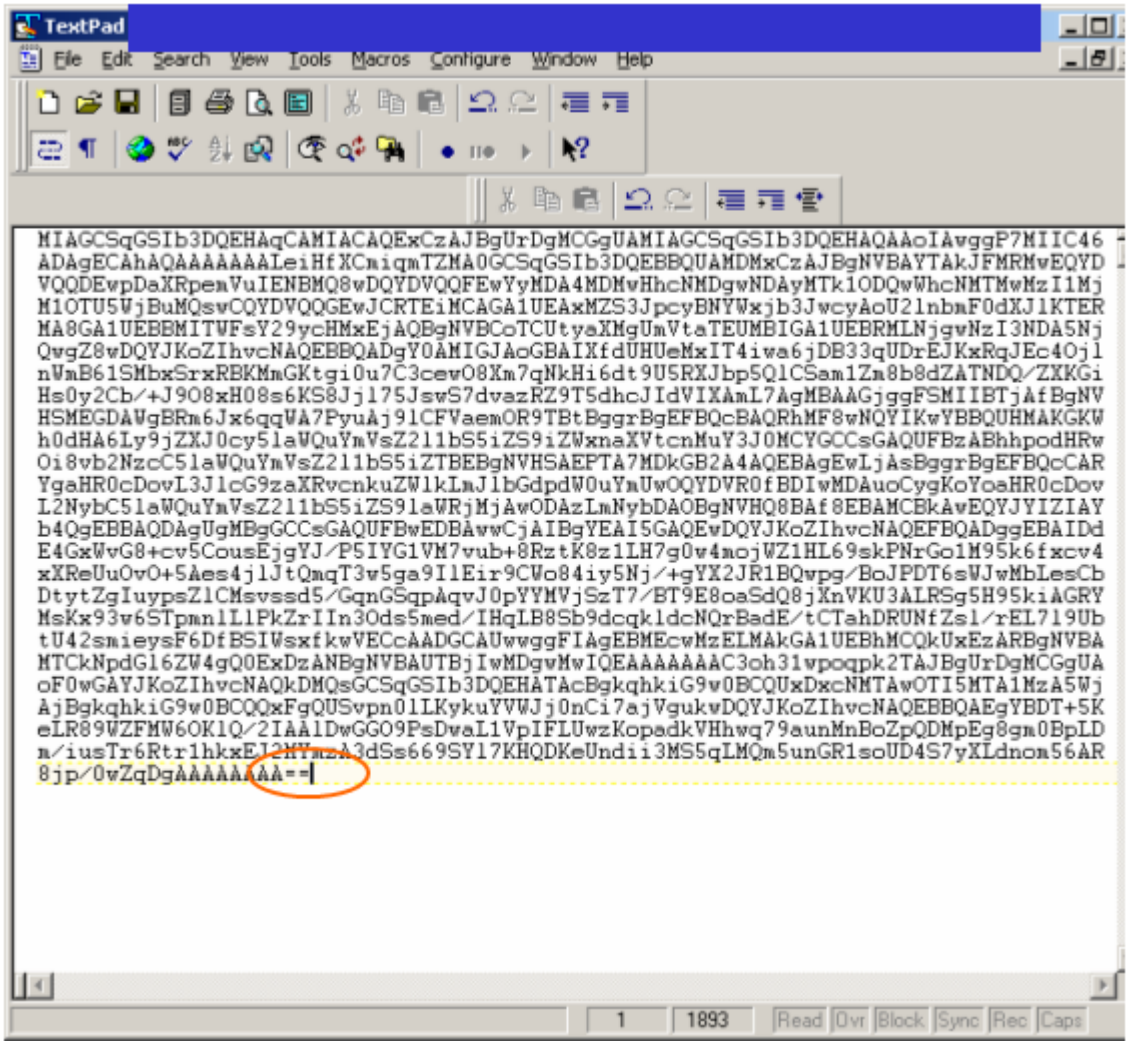
Attention: dès que vous avez créé votre fichier FS, vous ne pouvez plus changer votre fichier FI. Si vous modifiez encore votre fichier FI, vous devez recréer un nouveau fichier FS.

10. Les adaptations manuelles de votre fichier FS

Avant d'envoyer votre fichier, il y a encore quelques adaptations manuelles à faire dans le fichier FS.
Vous ouvrez le fichier FS avec un éditeur de texte comme Textpad ou Notepad.
Vous supprimez la première ligne (-----DÉBUT PKCS7-----) ainsi que la dernière ligne (-----END PKCS7-----).
Attention : le fichier FS ne peut pas contenir de lignes vierges à la fin du texte (supprimez éventuellement le retour chariot).



Voici le résultat de votre fichier FS



Après ces adaptations, sauvegardez le fichier FS avec la combinaison suivante [CTRL]+[S].