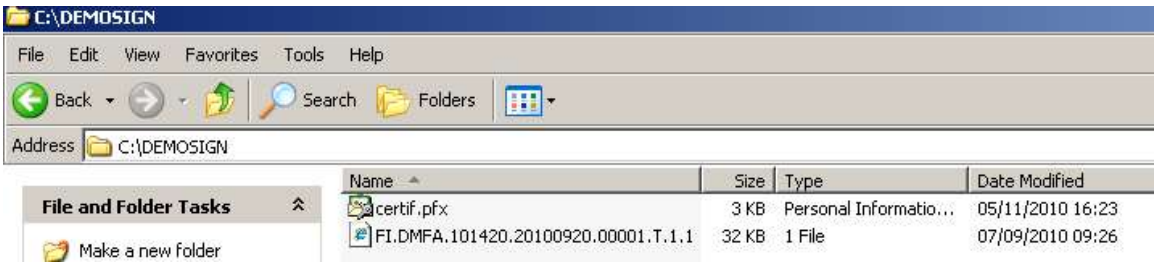
Générer un fichier de signature avec OpenSSL

Ce guide nécessite une installation fonctionnelle de OpenSSL 3. La procédure d'installation de cet outil diffère selon votre système d'exploitation et n'est pas documentée dans ce guide. Les commande OpenSSL reprises dans ce guide doivent être introduites dans l'invite de commande de votre système d'exploitation (Microsoft Windows est arbitrairement choisi comme exemple ci-après).

Choisissez un répertoire sur votre PC dans lequel vous installerez votre keystore (format PFX/P12) et votre fichier de déclaration (FI).



Dans la suite de ce guide, les noms suivants sont utilisés comme exemples :

- C:\DEMOSIGN : Le répertoire dans lequel se trouve le fichier de déclaration et votre keystore
- certif.pfx: Nom de votre keystore
- ww123 : mot de passe de votre keystore

OpenSSL ne permet pas de signer directement à partir du keystore PFX, nous allons donc extraire la clé privée et le certificat de votre keystore avant de procéder à la signature elle-même.

Extraction de votre certificat au format PEM

Pour extraire votre certificat de votre keystore PFX, veuillez exécuter la commande OpenSSL suivante :

```
openssl pkcs12 -in C:\DEMOSIGN\certif.pfx -passin pass:ww123 -out C:\DEMOSIGN\certificate.pem -nokeys
```

Extraction de votre clé privée au format PEM

Pour extraire votre clé privée de votre keystore PFX, veuillez exécuter la commande OpenSSL suivante :

```
openssl pkcs12 -in C:\DEMOSIGN\certif.pfx -passin pass:ww123 -passout pass:ww789 -out C:\DEMOSIGN\privatekey.pem -nodes -nocerts
```

Signature de votre fichier déclaration (FI)

Chaque fois que vous voulez envoyer un fichier FI, vous devez créer un fichier signature (FS) correspondant en utilisant la clé privée et le certificat extrait de votre keystore PFX.

Vous pouvez utiliser votre certificat et votre clé privée 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 extraire de nouveau ces éléments de votre keystore.

Vous pouvez maintenant créer votre **fichier de signature** en SHA256 en introduisant la commande OpenSSL suivante :

```
openssl cms -sign -md sha256 -signer C:\DEMOSIGN\certificate.pem -inkey
C:\DEMOSIGN\privatekey.pem -in C:\DEMOSIGN\FI.DMFA.123456.20120213.00001.T.1.1 -
binary -out C:\DEMOSIGN\FS.DMFA.123456.20120213.00001.T.1.1 -outform PEM
```

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.

Adaptations manuelles de votre fichier signature (FS)

Avant d'envoyer votre fichier, il y a encore quelques adaptations manuelles à faire dans le fichier FS. Veuillez ouvrir le fichier FS avec un éditeur de texte et supprimez la première ligne (-----BEGIN CMS-----) ainsi que la dernière ligne (-----END CMS-----).

Attention : le fichier FS ne peut pas contenir de lignes vierges à la fin du fichier (supprimez éventuellement le retour chariot).

Voici le résultat attendu de votre fichier FS, n'oubliez pas d'enregistrer vos modifications

```
MIIF9QYJKoZIhvcNAQcCoIIF5jCCBeICAQExDTALBglghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIDUTCCA00wggI1oAMCAQICCQCmlFf84mT2ezANBgkqhkiG9w0BAQUF
ADBNMR8wHQYDVQQDExZKb2huIFNtaXRoICh1ZXN0IDMwNzIpMQswCQYDVQQGEwJC
RTENMAsGA1UEKhMESm9objEOMAwGA1UEBBMFU2lpdGgwHhcNMjMwNjE5MTAwNzU3
WhcNMjMwNjIwMTAwNzU3WjBBMRMwEQYDVQQDEwpKb2huIFNtaXRoMQswCQYDVQQG
EwJCRTENMAsGA1UEKhMESm9objEOMAwGA1UEBBMFU2lpdGgwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCwMNmhnNzhNjzMYkHxafFx3edmmOJpIfVNejh0
8BEYO2y8vYUmA/IpUd9oQRTbLKyS29qQKROMC0zdxydq2iVGqKWeL2+ErYANqrQ0
lV2oRUVQilPYMfM3eN8J677/eRzlUwz8yMiZ9wo+Ojele4X2edFISWaStYWGEm8B
Csb47jKoioeh0ooDw4R6CSEQ4Ve+PdkZaH5OQAs+6m4KMiywAs82C6pCmZiJtWO8
l6FafNEGxUKFif69etYpQqYNp3Td6b8YqNjyFLvjBTQsvaDgPHYs57af37hOEVRo
vC/I5gKlcL+7cxBq6XYNtxH1+l/kmiNQZ3/ADFsV7VLyqMlbAgMBAAGjPDA6MB0G
A1UdDgQWBBSCVa23KIlF9y3TdRNtYdqZDF7hKzAMBgNVHRMBAf8EAjAAMAsGA1Ud
DwQEAwIGwDANBgkqhkiG9w0BAQUFAAOCAQEADIOVgx/nRpzEoh8+KcfIDnsvWYL2
ZDSlvelvRqbzYqBcq+vSa6V93x0tYEpDvF3zU3nHH5IrKkdnfdQKnyUh2fnyKJdC
iaf6LgT972b8QFoXQ0XbZmjRsu9KjxGMaSFRnvDOIOLtNFpFAo0Ch3JKt6zIENF7
5u0XAR8iA4mQW3TAwl5jL9Elm6Lclo9JRB/b79DxST4fbtDwRhXeQGOEvrqjjEa3
cuGkDxLYaXQUdK8m7xAl9k623SzJMMmkufTNu7ZF8SewrZg0Rd6Uk5+StafIvwEb
DCD+pZC0QulwIioE5+dmxzIy+7NmN40lHdVhKmcN0snBGRGy5hIH8b8tpTGCAmow
ggJmAgEBMFowTTEfMB0GA1UEAxMWSm9obiBTbW10aCAoVGVzdCAzMDcyKTELMAkG
A1UEBhMCQkUxDTALBgNVBCoTBEpvaG4xDjAMBgNVBAQTBVNtaXRoAgkAptRX/OJk
9nswCwYJYIZIAWUDBAIBoIHkMBgGCSqGSIb3DQEJAzELBgkqhkiG9w0BBwEwHAYJ
KoZIhvcNAQkFMQ8XDTIzMDYxOTE2MDMzMlowLwYJKoZIhvcNAQkEMSIEIAfyve80
7RbjoboNu35HuP2YHODMs+G/5WTYLEI8un5HMHkGCSqGSIb3DQEJDzFsMGowCwYJ
YIZIAWUDBAEqMAsGCWCGSAFlAwQBFjALBglghkgBZQMEAQIwCgYIKoZIhvcNAwcw
DgYIKoZIhvcNAwICAgCAMA0GCCqGSIb3DQMCAgFAMAcGBSsOAwIHMA0GCCqGSIb3
DQMCAgEoMA0GCSqGSIb3DQEBAQUABIIBAKRrjNLpjcg227MEylbuvWw45Ueu2zUp
nItbeAlo48tuDhZq2yB2OUufYYZ3E53QMEjsXqLe8rKpWjOoYNZRZj4jiKnQeYIF
6z7KKAmwBjcLvbJS5Yr4Aai4idtPTmT4o6gugULKcpxu5g7vad+yK08qEV4EbptH
AEJz9VaoSxhfghbu8teA6e3j7w7iflHa2mRxC+onDGf9wA0BUpsgSJvrtQyO3YIG
iMYL+Vfg/pDgSKo7ak9PTu3tQcwjh6cxm3PXnqStPZxlq8r5GSnlwwsot4Ftc0ml
AwQFW4yDbArSPL2CpRlBgaFRtyc7nUKCNKFE23UAlW5Gz8OAa+o5/pM=
```