Signature électronique de PDFs

Introduction

Mapping donne la possibilité de signer numériquement les fichiers PDFs générés. Pour cela, des certificats électroniques associés à des clés privés sont utilisés.

Prérequis

Il faut au préalable avoir à disposition un certificat et une clé privée.

Génération d'un certificat et d'une clé privé (pour notre exemple via openssl) :

```
openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:2048 -keyout private.pem -out certificate.cer
```

Clé privé : private.pem
Certificat : certificate.cer

Cette commande va permettre de générer un certificat et une clé privée dits "autogénérés" sans avoir recours à une autorité de certification. Cela n'a de sens que pour effectuer des tests. Pour un usage réel, il faudra obtenir un certificat par l'intermédiaire d'une autorité de certification (Certificate Authority, CA, AC).

Limites

- Le certificat est bien visible sur Foxit Reader mais non visible facilement sur Acrobat Reader.
- Mapping certifie les documents uniquement avec des signatures invisibles.

Reste à faire :

1. Vérifier qu'il soit bien visible si le certificat vient d'un organisme certifieur.
2. Valider le fonctionnement du pfx
3. Documentation le timestampurl(a priori il y a un bug sur cette fonctionnalité)

Remarque au sujet des certificats

Signature visible et invisible : Les différences

Apposer une signature numérique ajoute des métadonnées à un document sans modifier son contenu (et donc sans altérer son intégrité) : C'est ce qui

permet d’apposer plusieurs signatures à un document sans compromettre son intégrité.

- La signature visible inclut une métadonnée qui contient une marque visible (aspect de signature) lors de la lecture du document, indiquant qu’il a été signé.
- La signature invisible omet cette marque visible.

Pour rappel, Mapping gère uniquement les signatures invisibles.

Les deux types de signatures assurent l’intégrité du document. L’information du certificat numérique peut être vue dans les deux types lors de la validation d’une signature. Cependant, sur un document imprimé, seules les signatures visibles apparaissent. Ce type de signature peut être utile si des exemplaires imprimés de documents sont archivés.

De plus :

- Certifier (signature visible) : Appose une signature certifiée dans un champ de signature numérique existant (si disponible) ou à l’emplacement que vous désignez.
- Certifier (signature invisible) : Certifie le document, mais votre signature apparaît uniquement dans le panneau Signatures.

Le choix du type de signature peut dépendre des politiques de votre entreprise.

Différents types de certificats

MAPPING prend en charge plusieurs types de certificats

PFX

Un fichier PFX (ou PKCS#12) est un fichier qui contient à la fois la clé privée et le certificat X.509. La génération des demandes de signature de certificat (CSR, Certificate Signing Request) demeure un problème récurrent pour les clients. Avec un fichier PFX, le client n’a plus à créer son propre CSR. Une autorité de certification s’en charge pour lui de manière entièrement sécurisée pendant le processus de demande de certificat.

CSR

L’ autorité de certification (AC) utilisera les données de votre demande de signature de certificat pour créer votre certificat SSL. Voici une liste des informations clés :

1. Des informations sur votre entreprise et le site web que vous souhaitez sécuriser avec un certificat SSL. Elles comprennent :

Libellé	Description
Common Name (CN)(ex : *.exemple.fr www.exemple.fr mail.exemple.fr)	Le nom de domaine pleinement qualifié (FQDN) de votre serveur.

Organization (O)	La dénomination sociale de votre organisation. Veuillez ne pas utiliser d'abréviation et inclure la forme de l'entreprise, telle que « SA ».Pour les certificats EV et OV SSL, ces informations seront vérifiées par l'AC et incluses dans le certificat.
Organizational Unit (OU)	Le service de votre organisation responsable de la gestion du certificat.
City/Locality (L)	La ville où se situe votre organisation. Veuillez entrer le nom complet.
State/County/Region (S)	Le département ou la région où se situe votre organisation. Veuillez entrer le nom complet.
Country (C)	Le code à deux lettres du pays où se situe votre organisation.
Email Address	L'adresse e-mail du contact de votre organisation.

2. La clé publique qui sera incluse dans le certificat. Le SSL utilise la cryptographie à clé publique ou asymétrique pour chiffrer les données échangées lors d'une session SSL. La clé publique est utilisée pour le chiffrement et la clé privée correspondante est utilisée pour le déchiffrement des données.

3. Des informations sur le type et la longueur de clé. La longueur de clé la plus courante est RSA 2048 mais certaines AC acceptent des clés plus longues (ex : RSA 4096+) et les clés ECC.

Le CSR est généralement créé au format PEM encodé en Base64. Vous pouvez l'ouvrir avec un simple éditeur de texte

Il est possible d'avoir le certificat et la clé privée dans des fichiers séparés ou bien dans le même fichier

Dans des fichiers séparés

Voici un exemple d'un certificat et une clé privée dans deux fichiers séparés

Fichier private.pem

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFA
...
HRgFVVNXS8jTjAo2LL7U6rZK8gwsXWzqaXNLsvwj9HoF89+reRosTfIIk
-----END PRIVATE KEY-----
```

Fichier certificate.cer

```
-----BEGIN CERTIFICATE-----
MIID2TCCAsGgAwIBAgIJAKcd3Qk2E
...
bJVSEN4kV0mdg5jrFhCCZjrlumzs+MQ=
```

```
-----END CERTIFICATE-----
```

Dans le même fichier

Voici un exemple d'un certificat et d'une clé privée définis dans le même fichier **certifcle.pem**

Fichier certifcle.pem

Son contenu est une simple concaténation du contenu du fichier clé privé et du certificat.

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFA
...
HRgFVVNXS8jTjAo2LL7U6rZK8gwsXWzqaXNLsvwj9HoF89+reRosTfIIk
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIID2TCCAsGgAwIBAgIJAKcd3Qk2E
...
bJVSEN4kV0mdg5jrFhCCZjrlumzs+MQ=
-----END CERTIFICATE-----
```

Paramétrage

L'utilisation de la signature électronique au sein de MAPPING nécessite la copie de la clé privé et du certificat sur le serveur.
Son utilisation est alors possible dans les **workflows** MAPPING ou bien en ligne de commande via la commande **map_xps**

Copie des fichiers sur le serveur

Il faut mettre le fichier de la clé privé et le fichier du certificat sur le système de fichier de serveur

(Exemple : /apps/mapping/certificate)

Les différents paramètres

La signature électronique requiert l'utilisation de plusieurs paramètres.
Vous trouverez la liste dans le tableau ci-dessous :

Nom du paramètre	valeur	Signification
signclass	< 3	–
signdriver	VIDE	Signature électronique désactivée (les autres paramètres n'auront alors pas d'effet)

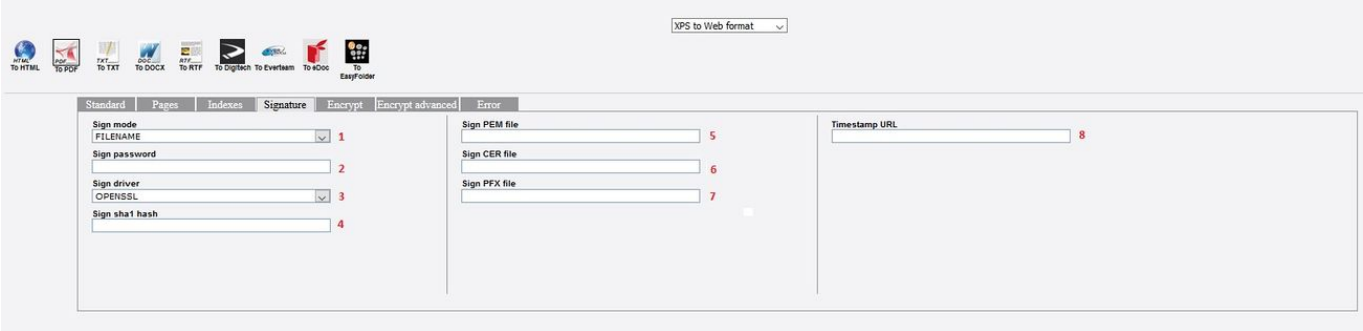
OPENSSL	Le mode OPENSSL est compatible avec toutes les plateformes supportées par Mapping. Il utilise un ou deux fichiers contenant les clés publiques et privées. Les fichiers doivent se trouver sur le serveur Mapping (chemins réseaux non supportés).	
FIRSTSIGNATURE	Le mode FIRSTSIGNATURE est valable uniquement sous Windows car il utilise un certificat installé sur le poste. Le certificat utilisé est le premier de la liste des certificats affichés dans Internet Explorer.	
WINDOWS	Activation du mode SHA1. Ceci est valable uniquement sous Windows car il utilise un certificat installé sur le poste. Le certificat utilisé est le défini par sa clé de hashage (empreinte numérique).	
signmode	FILENAME	A utiliser pour les signatures électroniques activées en mode OPENSSL
signpassword	Valeur de la passphrase du certificat	Utilisé dans le cas où le certificat contient une passphrase de sécurité
signsha1hash	Valeur du SHA1	utilisé si le paramètre **signdriver** est renseigné avec la valeur “WINDOWS”
signpemfile	Chemin complet du fichier de clé privé	Fichier de clé privée seul s’il est séparé du certificat ou fichier contenant à la fois la clé privée et le certificat
signcerfile	Chemin complet du fichier de certificat	Utilisé uniquement si le fichier du certificat est séparé du fichier de clé privée
signpfxfile	Chemin complet du fichier PFX	Utilisé uniquement pour les fichiers PFX (PKCS#12)
timestampurl	??	A documenter

Utilisation

Workflow

La boite des workflows MAPPING à utilisée est la boite **toPDF**. (XPS to web format / toPDF) De base, cette boite permet de générer un PDF à partir d'un fichier XPS. Cependant il est possible d'y paramétrer une signature électronique.

Onglet Signature



Cet onglet permet l'initialisation des paramètres listés dans le tableau des paramètres.

remarque : A noté que le workflow initialise le paramètre signclass à la valeur 0.

map_xps

Il est également possible d'utiliser la commande MAPPING de conversion **map_xps**

Il faudra alors initialiser les paramètres de signature électronique via des paramètres **-param:CLE=VALEUR**

Exemple :

```
"/apps/mapping/bin/map_xps" "-infile:/apps/mapping/infile/infile.xps" "-param:signmode=FILENAME" "-param:signclass=0" -param:signdriver=OPENSSL" "-param:signpemfile=/apps/mapping/certificate/private.pem" "-param:signcerfile=/apps/mapping/certificate/certificate.cer" "-toPDF" "-outfile:/apps/mapping/out/out.pdf"
```

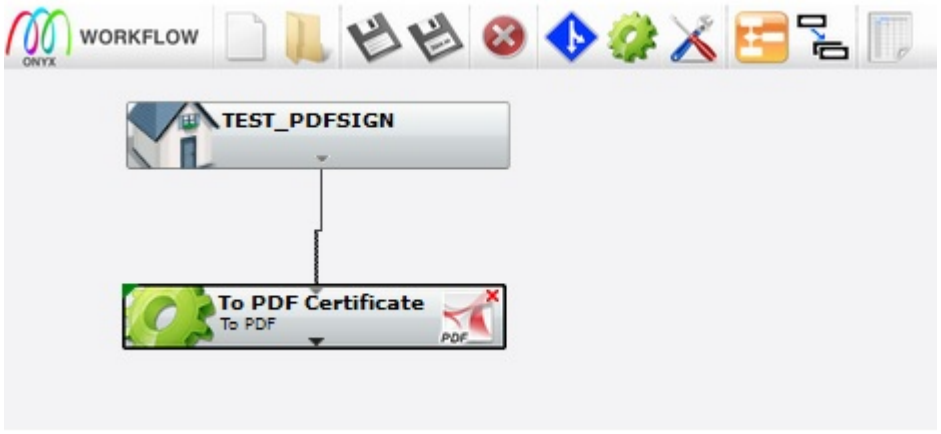
Exemples

Exemple 1

Dans cette exemple, nous allons voir comment convertir le fichier d'entrée (fichier XPS) en PDF en lui appliquant un certificat. Nous allons voir comment faire cela à travers d'un workflow et comment faire la même chose en ligne de commande.

Workflows

Création du worflow suivant :



Détail de la boite toPDF (Onglet standard) :

Détail de la boite toPDF (Onglet Signature) :

Ligne de commande sans profil de conversion

Exécutez la commande suivante :

```
"/apps/mapping/bin/map_xps" "-infile:/apps/mapping/infile/infile.xps" "-
param:signclass=0" "-param:signmode=FILENAME"
"-param:signdriver=OPENSSL" "-
param:signpemfile=/apps/mapping/infile/private.pem"
"-param:signcerfile=/apps/mapping/infile/certificate.cer" "-toPDF" "-
outfile:/apps/mapping/output/out.pdf"
```

Ligne de commande avec profil de conversion

Profil de conversion utilisé :

```
<pdf_signature>
   <label>for Adobe Reader</label>
   <language>PDF</language>
   <signclass>0</signclass>
   <signmode>FILENAME</signmode>
   <signpassword></signpassword>
   <signdriver>OPENSSL</signdriver>
   <signpfxfile></signpfxfile>
   <signpemfile>apps/mapping/infile/private.pem</signpemfile>
   <signcerfile>apps/mapping/infile/certificate.cer</signcerfile>
 </pdf_signature>
```

Exécuter la commande suivante :

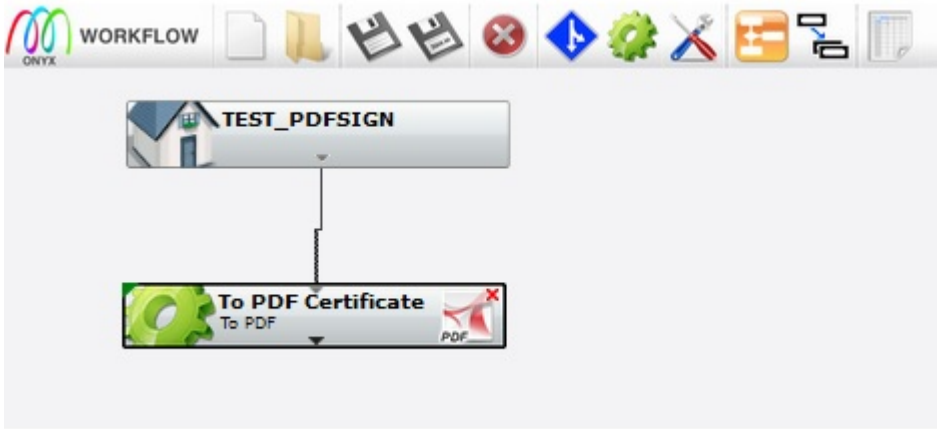
```
"/apps/mapping/bin/map_xps" "-infile:/apps/mapping/infile/infile.xps" "-
toPDF" "-outfile:/apps/mapping/output/out.pdf"
"-profile:pdf_signature"
```

Exemple 2

Dans cette exemple, nous allons voir comment utiliser un fichier contenant la clé privée et le certificat

Workflows

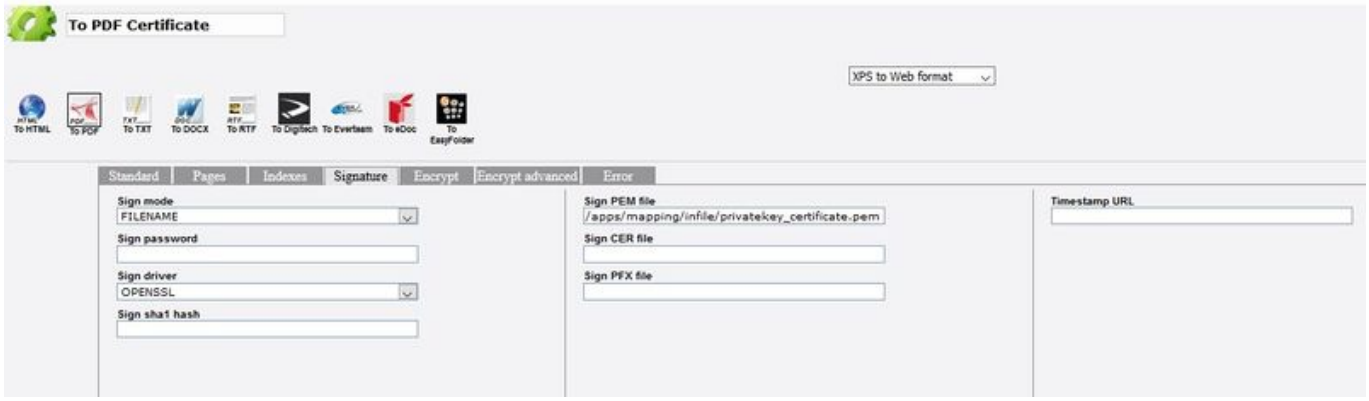
Création du worflow suivant :



Détail de la boite toPDF (Onglet standard) :

Détail de la boite toPDF (Onglet Signature) :

Le fichier ayant la clé privée et le certificat doit être mis dans le paramètre pem.



Ligne de commande sans profil de conversion

Exécutez la commande suivante :

```
"/apps/mapping/bin/map_xps" "-infile:/apps/mapping/infile/infile.xps" "-
param:signclass=0" "-param:signmode=FILENAME"
"-param:signdriver=OPENSSL" "-
param:signpemfile=/apps/mapping/infile/privatekey_certificate.pem" "-toPDF"
"-outfile:/apps/mapping/output/out.pdf"
```

Ligne de commande avec profil de conversion

Profil de conversion utilisé :

```
<pdf_signature>
   <label>for Adobe Reader</label>
   <language>PDF</language>
   <signclass>0</signclass>
   <signmode>FILENAME</signmode>
   <signpassword></signpassword>
   <signdriver>OPENSSL</signdriver>
   <signpfxfile></signpfxfile>
```

```
   <signpemfile>apps/mapping/infile/privatekey_certificate.pem</signpemfile>
   <signcerfile></signcerfile>
 </pdf_signature>
```

Exécuter la commande suivante :

```
"/apps/mapping/bin/map_xps" "-infile:/apps/mapping/infile/infile.xps" "-
toPDF" "-outfile:/apps/mapping/output/out.pdf"
"-profile:pdf_signature"
```

Liens externes

- https://helpx.adobe.com/fr/acrobat/using/validating-digital-signatures.html

Signature électronique Signature numérique, signature PDF