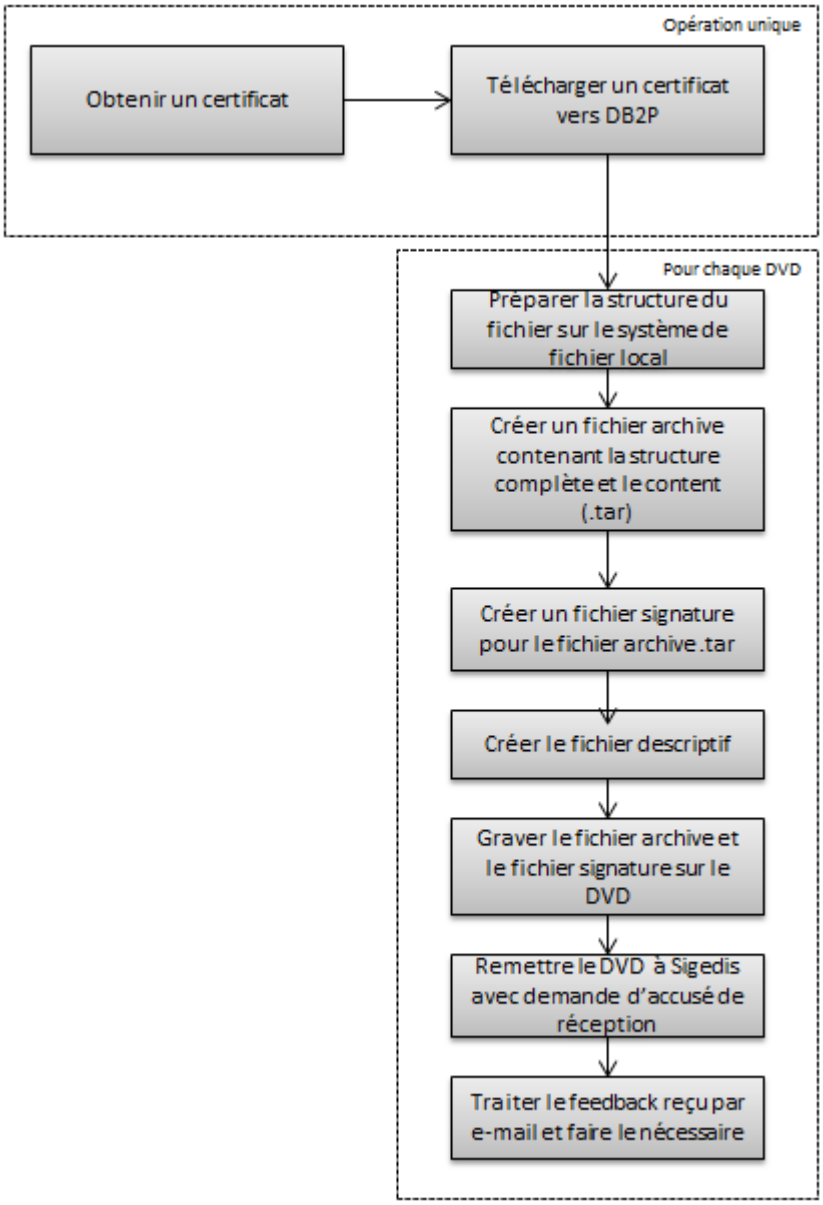
DB2P

PDF

Documentation technique

1. Procédure de création du DVD



1.1. Obtenir un certificat

Pour assurer un transfert sécurisé des données entre l'expéditeur et Sigedis, un système de sécurité « Public Key Infrastructure (PKI) » est utilisé. Il permet à Sigedis de vérifier l'identité de la source et assure qu'aucune donnée n'a été modifiée après que le DVD a quitté le bureau de l'expéditeur.

Pour être en mesure d'envoyer un DVD à Sigedis par ce canal, l'expéditeur doit d'abord obtenir une clé privée et une clé publique.

La procédure d'obtention du certificat et de signature du DVD est similaire à celle de l'envoi par batch de déclarations DB2P.

Deux types de certificats peuvent être utilisés :

- Le certificat présent sur la carte d'identité électronique du collaborateur travaillant pour l'expéditeur (méthode recommandée).
- Un certificat délivré par une autorité de certification

Il est recommandé de lire les documents suivants pour plus d'informations quant à l'obtention du certificat :

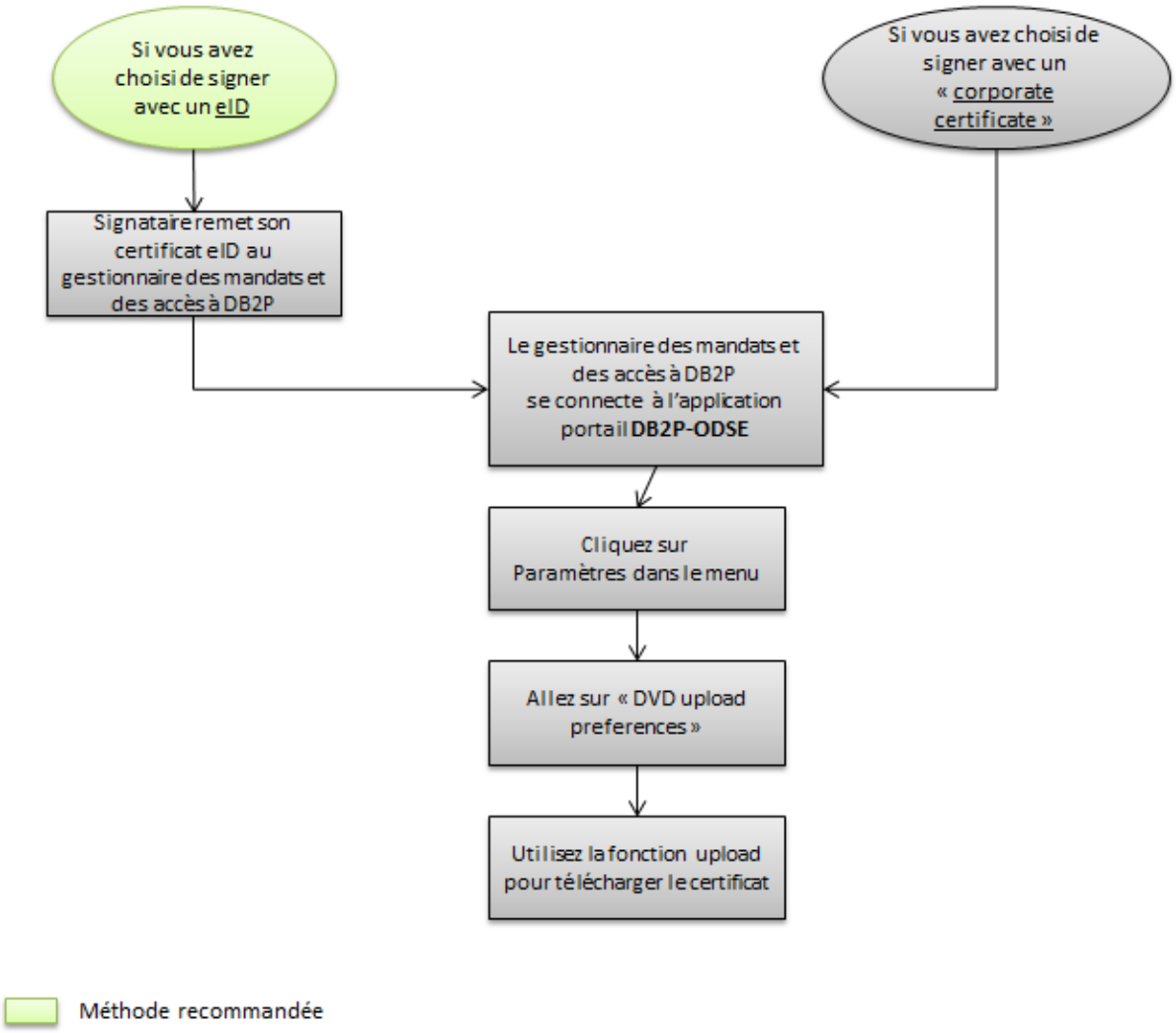
- Les deux types de certificat sont décrits ici :
  - Guide de démarrage du canal de transfert FTP → 2.2 Un certificat digital qualifié https://www.socialsecurity.be/site_fr/general/helpcentre/batch/document/pdf/manuel_d_utilisateur_ftp_F.pdf

- L'extraction d'une clé publique à partir de la carte d'identité électronique est décrite ici :
  - Procédure exportation du certificat de signature de la carte eID https://www.socialsecurity.be/public/doclibrary/fr/documents/pdf/Procedure_Certificat_Signature_F.pdf

Cependant, **le certificat ne peut pas être téléchargé vers le Portail de la Sécurité sociale comme décrit dans ces documents**. Pour des DVD, le système DB2P est responsable du stockage du certificat.

1.2. Upload du certificat vers DB2P (par l'utilisateur ayant le rôle « Gestion des mandats et accès à DB2P» -dénommé admin dans le schéma)

Sigedis a besoin de la clé publique pour être en mesure de vérifier la signature. Avant d'envoyer le premier DVD, l'expéditeur doit télécharger le certificat digital contenant cette clé via l'application **DB2P-ODSE** sur le site portail.



L'upload sera effectué par un utilisateur ayant le rôle « Gestion des mandats et accès à DB2P». A cet effet, si la méthode de signature choisie par l'expéditeur est la carte d'identité électronique, le signataire devra d'abord remettre son certificat à cet utilisateur. Cet utilisateur et le signataire sont dans ce cas deux personnes différentes. Toutefois, rien n'empêche que l'utilisateur ayant le rôle « Gestion des mandats et accès à DB2P» soit également le signataire. Ce choix est du ressort de l'expéditeur.

A ce stade, l'utilisateur ayant le rôle « Gestion des mandats et accès à DB2P» aura soit un certificat eID soit un certificat « corporate ». Ensuite, il se connectera dans l'application portail et utilisera l'option "Upload certificate" qui sera accessible dans le menu des paramètres.

Ces deux premières étapes ne sont exigées qu'une seule fois. Il n'y a qu'un seul cas où ces étapes devront être répétées : si l'expéditeur utilise la méthode du certificat eID pour signer le DVD et souhaite qu'ensuite un autre de ses collaborateurs puisse signer des DVD. Dans ce cas, le certificat de ce collaborateur doit également être téléchargé, et ce avant d'envoyer le DVD.

1.3. Préparer la structure du fichier

Le contenu du DVD doit être organisé comme suit :

- Les documents doivent être regroupés par régime
- Chaque groupe de documents (donc, pour chaque régime) doit être placé dans un **répertoire séparé**.
- Le nom du répertoire :

    - Doit être soit le SigedisId du régime (comme défini dans les instructions DB2P):

0000-0000-0000-0000-0000-0000

    - soit le couple “Registrant, RegistrantId”, séparé par le symbole “-“ (ce sont les mêmes règles qui valent pour le RegulationDefinition définies par les instructions DB2P) :

0000.000.000-*

1.4. Créer un fichier d’archive

Tous les répertoires doivent être rassemblés au sein d’un seul fichier d’archive. Ce fichier doit suivre ces directives-ci :

1. **Format** : TAR
2. **Filename** : le nom du fichier contient les parties suivantes :

    - Préfixe “DB2P_DVD”
    - Numéro BCE de l’expéditeur dans le format 10 chiffres sans séparateurs
    - La date de création du DVD dans le format AAAA-MM-JJ
    - Un suffixe pour distinguer divers DVD créés le même jour (format entier à partir de 1)

Toutes les parties sont séparées par le symbole “_”.

Un exemple de nom de fichier serait : “DB2P_DVD_0123456789_2012-02-17_1.tar”

3. Extension du fichier: “tar”
4. **Pas de compression** (pas de valeur ajoutée, étant donné que les PDF utilisent déjà une forme de compression).
5. **Pas de répertoire intermédiaire**: quand on décompresse le fichier d’archive dans un répertoire, les répertoires contenant les documents régime doivent apparaître à ce niveau. Il ne peut y avoir un répertoire entre. En d’autres termes, l’opération de compression devrait se faire en sélectionnant les répertoires de régimes et non un répertoire situé à un niveau supérieur que l’utilisateur aurait pu créer avant.

1.4.1. Pourquoi le format TAR?

Définition Wikipedia:

“Initially developed to be written directly to sequential I/O devices for tape backup purposes, **it is now commonly used to collect many files into one larger file for distribution or archiving**, while preserving file system information such as user and group permissions, dates, and directory structures.”

Le format a été choisi pour faciliter la procédure de signature (un seul fichier à signer).

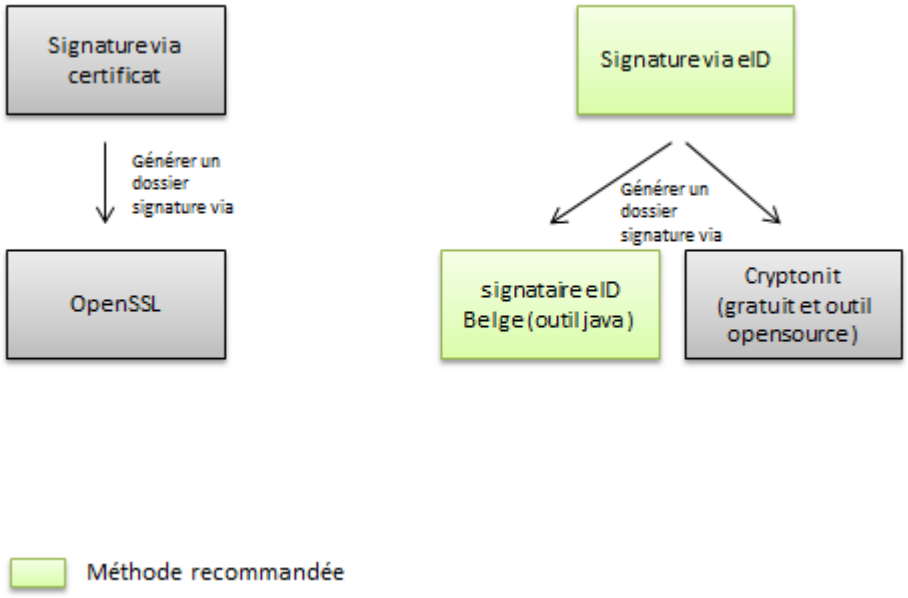
De nombreux outils de compression peuvent produire des fichiers d'archive TAR :

- 7zip (recommandé)
- Winzip
- Winrar
- ...

1.5. Signer le fichier d'archive

Signer le fichier d'archive entraîne la création d'un fichier de signature qui doit lui aussi être mis sur le DVD.

Il existe deux possibilités pour signer le fichier d'archive:



C'est à nouveau la même procédure que pour la transmission du batch DB2P. Les documents suivants expliquent la procédure :

- Signer avec la carte d'identité électronique (méthode recommandée) :
  - https://www.socialsecurity.be/public/doclibrary/fr/documents/pdf/Belgian_eIDSigner_Userguide_F.pdf
- Signer avec cryptonit :
  - https://www.socialsecurity.be/public/doclibrary/fr/documents/pdf/Manuel_Utilisateur_eID_Cryptonit_F.pdf
- Signer avec OpenSSL :
  - Guide de démarrage du canal de transfert FTP → 3.1 Le fichier de signature (FS) https://www.socialsecurity.be/site_fr/general/helpcentre/batch/document/pdf/manuel_d_utilisateur_ftp_F.pdf

L'extension du fichier de signature dépend de l'outil utilisé :

Tool	Extension
CryptonIt	.pem
Belgian eID signer	• No extension if input file is named "FI.xxx" • .b64 otherwise
OpenSSL	.pem

1.6. Créer le fichier descriptif (content.txt)

Le DVD doit également contenir un fichier descriptif avec les spécifications suivantes :

1. **Format** : txt
2. **Filename** : content.txt
3. **Location** : placé à la racine du DVD
4. **Content** : 3 « clé-valeur » (1 par ligne)
    - SENDERNAME : nom officiel de l'entreprise de l'expéditeur
    - SENDER : numéro d'entreprise ou numéro BCE dans le format 10-digit sans séparateurs
    - EMAIL : email de l'utilisateur qui a signé le fichier
    - DATE : Date de création dans le format YYYY-MM-DD

Exemple de fichier content.txt :

```
SENDERNAME=TestSender
SENDER=0123456789
EMAIL=john.smith@testsender.com
DATE=2012-02-17
```

1.7. Graver le DVD

1.7.1. Specifications du DVD

Le DVD doit satisfaire aux spécifications suivantes :

- Format : DVD+R, DVD-R (DVD-5 : Single Sided / Single Layer / Capacity : 4.7 GB)
- File system : Universal Disk Format (UDF) (v1.02, v1.50, v2.0x, v2.5, v2.6)

Lorsqu'on grave le DVD, une inscription doit être définie :

Label (inscription) : "DB2P_DVD_0123456789_2012-02-17_1"

1.7.2. DVD content

Après avoir été gravé, le DVD doit contenir 3 fichiers :

- Le fichier archive .tar
- Le fichier signature .xxx
- Le fichier descriptif «content .txt»

Les 3 fichiers sont localisés à la racine du DVD.

(*) l'extension du fichier signature dépend de l'outil utilisé (voir 1.5).

1.7.3. DVD inscriptions manuelles et label

Sur le disque, ainsi que sur la pochette, les informations suivantes doivent apparaître :

- SENDERNAME : nom officiel de l'entreprise de l'expéditeur
- SENDER : dans le format 10-digit sans séparateurs
- EMAIL : email de l'utilisateur qui a signé le fichier
- DATE : Date de création dans le format YYYY-MM-DD

1.8. Envoi du DVD à Sigedis (avec accusé de réception du courrier)

Une fois le DVD prêt, un membre du personnel de l'entité doit déposer physiquement le DVD dans les bureaux de Sigedis. Deux accusés de réception (un pour l'entité qui envoie et l'autre pour Sigedis) seront signés par un membre du personnel Sigedis. Attention: soyez certain de déposer le DVD chez Sigedis au 7e étage de la Tour du Midi et non à la réception (rez-de-chaussée).

Sigedis Zuidertoren 7de verdieping Ter attentie van Zineb Laksiri Europa Esplanade 1 1060 Brussel	Sigedis Tour du Midi 7e étage A l'attention de Zineb Laksiri Esplanade de l'Europe 1 1060 Bruxelles

1.9. Gérer le feedback de Sigedis

Sigedis validera le contenu du DVD et un rapport au format xml sera renvoyé à l'expéditeur par e-mail. Le feedback suivant sera délivré :

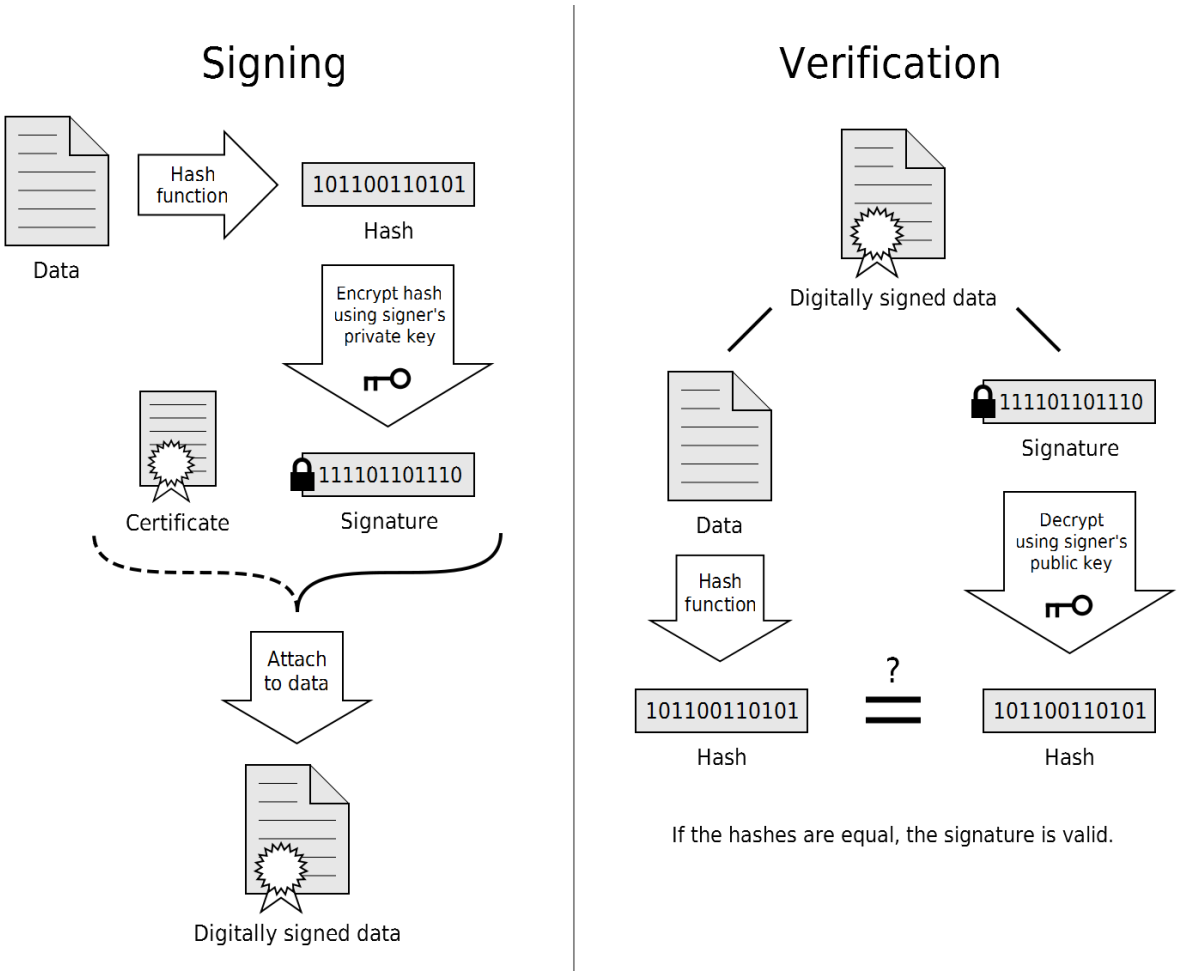
- Pour chaque fichier qui a *passé* les *contrôles de validation*, il y aura une confirmation de statut confirmant ceci.
- Pour chaque fichier qui a *échoué aux contrôles de validation*, une liste d'anomalies avec leurs explications sera fournie.
- S'il y a un problème avec le DVD même, des anomalies spécifiques seront également signalées.

Si le rapport contient des anomalies, l'expéditeur devra renvoyer le fichier concerné par plusieurs anomalies. Ceci peut se faire de différentes manières :

- En utilisant un nouveau DVD (ce nouveau DVD ne doit pas mentionner qu'il est un DVD correctif d'un DVD précédent)
- upload via batch (correction)
- upload via l'application portail (correction)

2. Appendice : signatures électroniques

Fondements de la signature électronique



Source : http://en.wikipedia.org/wiki/Electronic_signature