1. Choisir votre certificat digital qualifié

Chaque fichier de déclaration que vous envoyez par SFTP doit être accompagné d'un fichier de signature. Pour générer ce fichier de signature vous avez besoin d'un certificat digital qualifié.

Plusieurs choix s'offrent à vous :

1. Le certificat de **signature** de votre carte d'identité électronique (eID) (http://eid.belgium.be/fr/)

2. Un certificat digital qualifié du prestataire de services de certification suivant :
   GlobalSign : PersonalSign 3 pro
   (https://www.globalsign.eu/personalsign/personalsign3-pro/)

Comme la procédure de demande auprès d'un prestataire de services de certification peut prendre plusieurs jours, nous vous recommandons de vous y prendre bien à l'avance.

Ce certificat digital qualifié sera utilisé pour 2 actions :

- Vous devrez charger la clé publique de votre certificat digital qualifié (portant l'extension .cer) lors de la création de votre canal SFTP sur le site portail de la sécurité sociale (www.securitesociale.be).

- Sur la base de votre certificat qualifié (extension .pfx ou .p12) et pour chaque fichier de déclaration (FI), vous devrez créer un fichier de signature (FS) que vous placerez sur le serveur SFTP avec le fichier de déclaration.

Remarques importantes sur le choix de votre certificat

Il est important, lors du choix d'un certificat digital qualifié, de tenir compte de la manière dont vous comptez créer vos fichiers de signature (FS) :

Vous pouvez créer vous-même votre fichier de signature, en utilisant par exemple OpenSSL, ou utiliser des programmes que des producteurs de logiciels ou vous-même auraient développé.

Procédure OpenSSL :

Si vous souhaitez créer le fichier de signature par le biais de OpenSSL, il est important de demander un certificat à votre prestataire de services de certification, à partir duquel vous pourrez ensuite exporter la clé privée. Ceci pose problème pour les certificats figurant sur des cartes à puce ou des clés USB.
En effet, la procédure décrite dans la partie 10 Annexe : Générer un fichier de signature (FS) via OPENSSL ne convient PAS aux certificats qui se trouvent sur une carte d'identité électronique (eID) ou sur une carte Isabel. Dans la pratique, la procédure ne peut être utilisée que pour des certificats émis par Globalsign.

Apposer sa signature avec la carte d'identité électronique (eID) :

Si vous voulez créer un fichier de signature avec l'eID, vous pouvez utiliser la procédure avec **Cryptonit**. Consultez la procédure avec Cryptonit dans la bibliothèque de documents complémentaires (https://www.socialsecurity.be/public/doclibrary/fr/batch.htm). Vous pouvez bien entendu développer vous-même les programmes nécessaires ou faire appel à des logiciels disponibles sur le marché.

La procédure avec Cryptonit exige la présence du titulaire de l'eID.
Pour chaque fichier de signature, l'eID devra être
insérée dans le lecteur de carte et le titulaire de l'eID devra saisir son code PIN. Par conséquent, si le titulaire de l'eID est absent et que vous devez créer un fichier de signature pour l'envoi d'un message structuré, vous devrez utiliser une autre eID. Avant l'envoi, votre gestionnaire local ou co-gestionnaire local devra alors charger la clé publique de l'autre eID dans les paramètres de votre canal sur le site portail.

Apposer sa signature avec la carte Isabel :

Construire un fichier de signature sur base d'une carte Isabel **n'est pas possible** parce que la clé privée ne peut pas être exportée. Nous ne sommes donc pas en mesure de vous fournir un manuel ou une technique pour le faire. Le helpdesk de chez Isabel ne sait pas vous aider non plus.