Uw gekwalificeerd digitale certificaat kiezen.

Elk aangiftebestand dat u via SFTP verzendt moet vergezeld zijn door een handtekeningbestand. Om dit handtekeningbestand aan te maken heeft u een gekwalificeerd digitaal certificaat nodig.

U kan kiezen tussen:

1. Het handtekeningcertificaat (**Signature**) van uw elektronische identiteitskaart (eID) (http://eid.belgium.be/nl/)

2. Een gekwalificeerd digitaal certificaat van de volgende certificatiedienstverlener:
   GlobalSign: PersonalSign 3 pro
   (https://www.globalsign.eu/personalsign/personalsign3-pro/)

Aangezien de aanvraagprocedure bij een certificatiedienstverlener verschillende dagen in beslag kan nemen, raden we u aan dit voldoende ruim op voorhand te doen.

U zal uw gekwalificeerd digitale certificaat voor 2 acties moeten gebruiken.

- U zal de publieke sleutel van uw gekwalificeerd digitaal certificaat (met de extensie .cer) moeten opladen bij het aanmaken van uw SFTP-kanaal op de portaalsite van de sociale zekerheid (www.socialezekerheid.be).

- U zal op basis van uw gekwalificeerd certificaat (extensie .pfx of.p12) en voor elk aangiftebestand (FI) een handtekeningbestand (FS) moeten aanmaken dat u samen met uw aangiftebestand op de SFTP-server plaatst.

Belangrijke opmerkingen bij de keuze van uw certificaat:

Bij de keuze van een gekwalificeerd digitaal certificaat is het belangrijk om rekening te houden met de wijze waarop u uw handtekeningbestanden (FS) gaat aanmaken:

U kan uw handtekeningbestanden zelf aanmaken via bijvoorbeeld OpenSSL of u kan gebruik maken van programma's die door softwareproducenten of door uzelf zijn ontwikkeld.

OpenSSL-procedure:

Indien u het handtekeningbestand via OpenSSL wenst aan te maken is het belangrijk dat u aan uw certificatiedienstverlener een certificaat vraagt waarvan u de private sleutel kan exporteren. Bij certificaten die zich op chipkaarten of USB-sleutels bevinden vormt dit een probleem.
Dit houdt in dat de in de stap 'FS-bestand aanmaken met OPENSSL' beschreven procedure NIET geschikt is voor certificaten die zich bevinden op een elektronische identiteitskaart (eID) of op een Isabelkaart. In de praktijk is de procedure enkel bruikbaar voor certificaten van Globalsign.

Handtekenen met de elektronische identiteitskaart (eID):

Indien u met de eID een handtekeningbestand wenst aan te maken kan u gebruikmaken van de procedure met behulp van **Cryptonit**. U kan de procedure met Cryptonit vinden in de bibliotheek met complementaire documenten (https://www.socialsecurity.be/public/doclibrary/nl/batch.htm). U mag uiteraard ook zelf de nodige programma's ontwikkelen of een beroep doen op softwarepakketten die op de markt beschikbaar zijn.

De beschreven procedure met behulp van Cryptonit vereist dat de eigenaar van de eID aanwezig is.

Bij ieder handtekeningbestand zal de eID in de kaartlezer moeten zitten en zal de eigenaar van de eID zijn pincode moeten ingeven. Dit impliceert dat als de eigenaar van de eID niet aanwezig is, en u voor een verzending van een gestructureerd bericht een handtekeningbestand moet aanmaken, u een andere eID zal moeten gebruiken. Alvorens te verzenden zal uw lokale of co-lokale beheerder in dat geval de publieke sleutel van de andere eID moeten opladen bij de instellingen van uw kanaal op de portaalsite.

Handtekenen met een Isabelkaart:

Het aanmaken van een handtekeningbestand op basis van een Isabelkaart is **niet mogelijk** omdat de private sleutel niet geëxporteerd kan worden. Wij kunnen u hiervoor geen handleiding of techniek aanbieden. Ook de helpdesk van Isabel kan u hierbij niet helpen.