Beroepscertificaat

In de elektronische communicatie is het niet mogelijk om een ‘natte’ handtekening te gebruiken. De wet (Burgerlijk Wetboek Boek 3, artikel 15a) biedt in deze de mogelijkheid om een elektronische handtekening te gebruiken die dezelfde rechtsgevolgen heeft als een handgeschreven handtekening. Een elektronische handtekening komt tot stand met een digitaal certificaat dat daartoe specifiek gekwalificeerd is. In Nederland is dat het PKIoverheid (persoonsgebonden) beroepscertificaat.

Beroepscertificaten zijn alleen voorbehouden aan beoefenaars van een erkend beroep, zoals Accountant-Administratieconsulent en registeraccountant. In tegenstelling tot de PKIoverheid server services-certificaten die uw organisatie gebruikt voor het versturen van SBR-berichten (zoals jaarrekeningen en fiscale aangiften) bent u als individu zowel abonnee- als certificaathouder. Dit betekent dat alleen uzelf het certificaat kunt aanvragen en dat u zelf verantwoordelijk bent voor het beheer ervan.

Met het beroepscertificaat kan de ontvanger van het elektronisch bericht onomstotelijk vaststellen welke persoon dit bericht ondertekend heeft en dat deze persoon bevoegd is om zijn werkzaamheden uit te voeren. In het geval van een AA of RA betekent dat dat hij ingeschreven staat in het accountantsregister.

Toepassingsgebieden

Indien u een op SBR gebaseerde elektronische accountantsverklaring afgeeft bij een jaarrekening, dan dient u de verklaring elektronisch te ondertekenen. Dit doet u dan met het PKIoverheid-beroepscertificaat. Naast het ondertekenen is het ook noodzakelijk dat u met hetzelfde beroepscertificaat de SBR-jaarrekening waarmerkt.

De banken, verenigt in het Financiële Rapportages Coöperatief (FRC), hebben aangegeven dat de SBR-kredietrapportages in de toekomst voorzien moeten worden van een begeleidende samenstelverklaring. Deze samenstelverklaring dient dan, gelijk aan de elektronische jaarrekening met controleverklaring, eveneens te worden getekend met het PKIoverheid-beroepscertificaat. Op dit moment is er nog sprake van een overgangsregeling, waardoor u bij het aanleveren van kredietrapportages geen verklaring afzonderlijke aanlevert. U heeft dus nog geen beroepscertificaat nodig heeft.

Aanschaf PKIoverheid-beroepscertificaat

Door de NBA zijn de volgende partijen (Trusted Service Providers) gemachtigd voor het leveren van beroepscertificaten:

- Digidentity B.V.
- KPN Corporate Market BV
- Quo Vadis Trustlink BV
- CreAim (dealer van KPN certificaten)

Indien u een beroepscertificaat wenst aan te schaffen, dan dient u contact op te nemen met één van de bovenstaande TSP's. Zij zullen u informeren over het proces van het aanschaffen en het in gebruik nemen van een beroepscertificaat.

Bij de aanschaf van een PKIoverheid-beroepscertificaat dient u er mee rekening te houden dat een beroepscertificaat uit drie delen kan bestaan. Elk deel van het beroepscertificaat heeft zijn eigen toepassingsgebied:

1. Onweerlegbaarheid
2. Authenticiteit
3. Vertrouwelijkheid

Voor het digitaal aanleveren van een jaarrekening en de toekomstige kredietrapportage heeft u alleen het eerste deel nodig. Dit betreft het deel 'onweerlegbaarheid' waarmee u in staat bent om een elektronische gekwalificeerde handtekening te zetten.

Voordat tot uitgave van een certificaat wordt overgegaan zal de TSP eerst bij de NBA controleren of u als AA of RA ingeschreven staat in het accountantsregister en eventueel certificeringsbevoegd bent. Indien er na uitgifte van een certificaat sprake is van een (tijdelijke) doorhaling of uitschrijving dan zal de NBA dit melden aan de desbetreffende TSP, die op haar beurt het beroepscertificaat intrekt.

Extern beheer

De meest voorkomende variant voor de uitgifte van een persoonsgebonden beroepscertificaat is de uitgifte op een hardware token (bijvoorbeeld een USB dongel). Over de deze hardware token heeft u als verkrijger de volledige beschikking. Bij wijze van spreken kan een hardware token altijd in de binnenzak worden meegenomen en indien gewenst door u worden vernietigd.

Met de nieuwe Europese eIDAS verordening zijn de eisen veranderd. De eIDAS verordening maakt het ook mogelijk dat gekwalificeerde certificaten extern mogen worden opgeslagen. Het voordeel van een externe opslag is dat de gebruiker van het certificaat niet continue fysiek over een token hoeft te beschikken om zijn elektronische handtekening te zetten. Het certificaat is in dit geval opgeslagen op daarvoor speciale bestemde hardware dat via een externe connectie bereikbaar is.

Aan het opslaan van gekwalificeerde certificaten in een Cloud omgeving zijn overigens strikte voorwaarden verbonden. De externe omgeving moet volledig worden beheerd door een gekwalificeerde dienstverlener. Wie gekwalificeerde dienstverleners mogen zijn, wordt bepaald door het Agentschap Telecom. De gekwalificeerde dienstverleners moeten geaccrediteerd zijn en staan onder continue toezicht van het Agentschap Telecom. Dienstverleners die hiervoor in aanmerking komen zijn de huidige certificaatleveranciers (Digidentity, KPN Corporate Market BV en Quo Vadis Trustlink BV). Het is bij de NBA nog niet bekend welke van deze leveranciers geaccrediteerd zijn voor het externe beheer en of zij externe beheer oplossingen gaan aanbieden.