



## Verzamelcertificaten SBR

Hieronder enkele aandachtspunten vanuit juridisch oogpunt ten aanzien van het gebruik van verzamelcertificaten:

- De dienstverlener dient als certificaathouder te voldoen aan de eisen die het PKIoverheid-stelsel aan hem stelt en de verplichtingen jegens zijn *certificate service provider* (CSP).
- De dienstverlener die zijn certificaat ter beschikking stelt voor gebruik door klanten, zal daarnaast moeten voorzien in de nodige waarborgen om te reguleren (afbakenen) wie – en voor welk gebruik – toegang heeft tot het certificaat.
- Ook zal hij moeten voorzien in de nodige waarborgen om te kunnen vastleggen en aantonen wie, wanneer, hoe, waarvoor het certificaat gebruikt.
- Door zijn certificaat voor gebruik ter beschikking te stellen is de dienstverlener een schakel in de keten van elektronisch bestuurlijk verkeer. Hij is daarom, net als de andere betrokken partijen in de keten, verantwoordelijk voor het nemen van maatregelen (organisatorisch, technisch, ...) voor voldoende betrouwbaarheid en vertrouwelijkheid van de informatie-uitwisseling.
- Bij het opvragen van SBA's (serviceberichtsanslagen) is gebruik van een verzamelcertificaat niet toegestaan. Daarvoor is een certificaat van de fiscale dienstverlener zelf nodig. Het gebruik van een verzamelcertificaat biedt
- namelijk onvoldoende waarborgen voor het beschikbaar stellen van gevoelige (persoons)gegevens.

Daarnaast een aantal praktische aandachtspunten ten aanzien van het gebruik van verzamelcertificaten:

Bij gebruik van een verzamelcertificaat neemt de dienstverlener de facto een gedeelte van verantwoordelijkheid van de intermediair over. Dit gedeelte zal de dienstverlener dus zelf moeten regelen.

Praktisch gezien moet de dienstverlener er voor zorgen dat gebruik van zijn verzamelcertificaat is gereguleerd (niet iedereen kan er zomaar gebruik van maken) en het gebruik is te relateren aan geautoriseerde organisaties (personen).

Voor een ingestuurd bericht zal namelijk als worden gekeken naar het gebruikte certificaat. Als de organisatie niet zelf heeft aangeleverd maar voor een ander (o.b.v. inhoud van het bericht) en er ontstaat discussie over de inhoud van het bericht, dan is het aan te bevelen dat de dienstverlener kan aantonen wie het bericht dan daadwerkelijk heeft aangeleverd. Praktisch gezien kan dit op basis van logging binnen de applicatie (vastleggen wie, wanneer, welk bericht heeft aangeleverd. Dit gecombineerd met een autorisatielijst van gebruikers).

De dienstverlener moet dus naast technisch een aantal waarborgen inbouwen, veelal vanuit eigen belang ook zijn voorwaarden aanpassen. In de voorwaarden legt de dienstverlener dan weer een gedeelte van de verantwoordelijkheid bij gebruik van de applicatie (en daarmee het certificaat) bij de eindgebruiker. Op die manier kan een sluitend geheel worden opgebouwd.

Belangrijk is wel in de voorwaarden vast te leggen voor welke dienstverlening dit nu wordt geregeld (dus SBR proces xyz of bijv. Digipoort). Afhankelijk van het proces kunnen namelijk er andere handelingen worden gedaan en kan het belang van een certificaat (en de waarde van de handtekening en daarmee aansprakelijkheid) variëren.