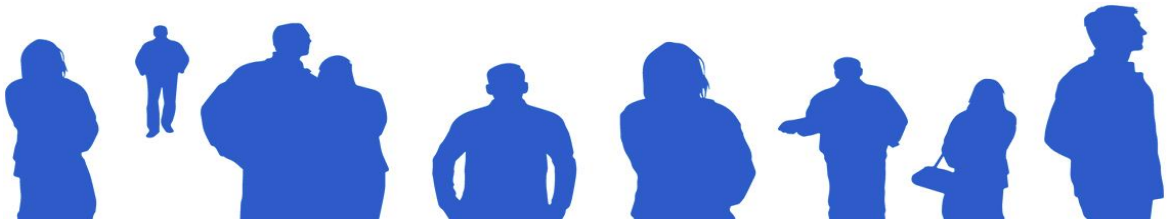


Authenticatie in de BRP

implementatieteambrp@operatiebrp.nl

Actualisatiedatum: 1 mei 2017

	Toelichting op wijziging
Wijziging t.o.v. versie 1.0	Digikoppeling 3.0 is vervangen door Digikoppeling 2.0. Meer informatie is te vinden op: www.operatiebrp.nl/afnemers/digikoppeling
Wijziging t.o.v. versie 1.1	De term 'abonnement' is vervangen door 'leveringsautorisatie'
	Rol Transporteur en rol Ondertekenaar is toegevoegd aan de toelichting op de typen aansluiting op de BRP

Notitie

1. Inleiding

Deze notitie beschrijft de wijze waarop authenticatie in de centrale BRP-voorzieningen (vanaf hier 'de BRP') geregeld wordt en welke vereisten dit stelt aan een afnemer om aan te kunnen sluiten op de BRP. Deze notitie is bedoeld voor **afnemers *niet zijnde gemeenten*** en is zowel van toepassing op afnemers die rechtstreeks aansluiten op de BRP als op afnemers die gebruik maken van een bewerker[1] in de aansluiting op de BRP.

In het volgende hoofdstuk volgt een uitleg van de technische oplossing voor authenticatie in de BRP. Om als afnemer te kunnen bepalen op welke wijze authenticatie voor de eigen aansluiting(en) ingeregeld moet worden, is uw type aansluiting van belang. Specifiek gaat het daarbij om de wijze waarop een afnemer de directe communicatie in technische zin met de BRP gaat realiseren. In hoofdstuk 3 zijn deze verschillende type aansluitingen opgenomen.

2. Authenticatie van Partijen, de oplossingsrichting toegelicht

De BRP ontvangt en levert uitsluitend berichten van en aan juridisch geautoriseerde afnemers. Een juridisch geautoriseerde afnemer is de partij aan wie één of meer autorisatie(s) is/zijn verleend. Geautoriseerde partijen kunnen rechtstreeks communiceren met de BRP. In dat geval zet de geautoriseerde partij zelf de communicatie met de BRP op. Geautoriseerde partijen kunnen er ook voor kiezen om een bewerker in te schakelen voor de communicatie met de BRP. In dat geval machtigt een geautoriseerde partij deze bewerker om namens zijn organisatie de communicatie met de BRP op te zetten. De geautoriseerde partij blijft te allen tijde verantwoordelijk voor de aansluiting op en de opvraag van gegevens uit de BRP.

2.1 Communicatie & rollen in de BRP

Communicatie met de BRP volgt de Digikoppeling 2.0 standaard. Binnen deze standaard is gedefinieerd dat partijen zich identificeren met PKIoverheid-certificaten (PKIO-certificaten). Hierbij wordt onderscheid gemaakt naar een:

- Certificaat voor de versleuteling (encryptie) van de communicatie;
- Certificaat voor de ondertekening (signing) van het bericht.

In de communicatie met de BRP worden de volgende rollen onderkend:

- De Transporteur; voor het opzetten van een versleutelde verbinding.
- De Ondertekenaar; voor het digitaal ondertekenen van berichten.

[1] Voor de term 'bewerker' kunt u ook lezen: serviceorganisatie, connector, intermediair, gegevensbewerker.

In de berichtuitwisseling met de BRP wordt onderscheid gemaakt tussen de volgende vormen van communicatie:

- **Synchrone communicatie**
  De afnemer doet (via een bewerker) een verzoek aan de BRP: 'request-response'-berichten zoals bevraging of synchronisatieverzoek. Voor deze vorm van communicatie moet voldaan worden aan het Digikoppeling-profiel WUS: '2W-be-S'.
- **Asynchrone communicatie**
  De BRP informeert de afnemer (via de bewerker): 'push'-berichten zoals mutatie- en vulberichten. Voor deze vorm van communicatie moet voldaan worden aan het Digikoppeling-profiel EbMS: 'osb-rm-s'.

De berichten moeten worden verstuurd via een versleutelde TLS-verbinding. TLS is een protocol voor het opzetten en gebruiken van een beveiligde, versleutelde verbinding tussen twee computersystemen.

Vóór aansluiting op de BRP moeten IP-adressen uitgewisseld worden met de toekomstig beheerder van de BRP (Rijksdienst voor Identiteitsgegevens):

- Sluit een geautoriseerde partij rechtstreeks aan op de BRP? Dan wisselen de geautoriseerde partij en Rijksdienst voor Identiteitsgegevens IP-adressen uit.
- Sluit een geautoriseerde partij via een bewerker aan op de BRP? In dat geval wisselen de bewerker en Rijksdienst voor Identiteitsgegevens IP-adressen uit.
- Indien de geautoriseerde partij gebruik maakt van asynchrone communicatie wordt ook het IP-adres van de ontvangstservice uitgewisseld (het zogenaamde *endpoint*).

2.2 Machtigingen in de BRP

Indien een geautoriseerde partij voor de communicatie met de BRP een bewerker inschakelt, is het mogelijk om een bewerker te machtigen:

- Alleen voor de rol van Transporteur; in dat geval neemt de bewerker alleen de versleutelde verzending van berichten voor zijn rekening.
- Alleen voor de rol van Ondertekenaar; in dat geval neemt de bewerker alleen de ondertekening van berichten voor zijn rekening.
- Voor beide rollen - Transporteur en Ondertekenaar; in dat geval neemt de bewerker zowel de versleutelde verzending als de ondertekening van berichten voor zijn rekening.
- Indien een geautoriseerde partij een bewerker machtigt voor de rol van Ondertekenaar, dan moet een extra machtiging afgeven worden aan de bewerker om toegang te geven tot de diensten binnen het koppelvlak Leveren (waarvan de geautoriseerde partij gebruik maakt).

De geautoriseerde partij geeft de machtiging(en) aan Rijksdienst voor Identiteitsgegevens door. Machtigingen en de gemachtigde partijen worden binnen de BRP geregistreerd. Bij het opzetten van de communicatie en de verwerking van binnenkomende berichten valideert de BRP of sprake is van een geldig PKIO-certificaat en een geldige machtiging. Indien een bewerker is gemachtigd voor beide rollen, kan hetzelfde PKIO-certificaat gebruikt worden voor de ondertekening én het versleuteld verzenden van het bericht. Dit is echter alleen mogelijk indien de TLS-afhandeling voor het versleuteld verzenden op dezelfde (proxy)server met dezelfde Certificate Name (CN) gebeurt[2].

2.3 Identificatie in de BRP

In de BRP worden geautoriseerde partijen en bewerkers als partij geregistreerd. Voor de identificatie van geregistreerde partijen en machtigingen in de BRP wordt het OverheidsIdentificatieNummer (OIN) gebruikt. Dit OIN[3] is opgenomen in het PKIO-certificaat. Een geautoriseerde partij of bewerker moet altijd zijn eigen PKIO-certificaat inclusief unieke OIN[4] gebruiken in de communicatie met de BRP.

Indien een geautoriseerde partij een bewerker machtigt, dan stelt deze partij nooit zijn eigen PKIO-certificaat ter beschikking aan zijn gemachtigde bewerker.

---

[2] Raadpleeg het document 'Gebruik en Achtergrond Digikoppeling Certificaten' van Logius voor meer informatie.
[3] Een OIN wordt toegekend door Logius. Nadat het OIN is verkregen kan bij één van de aangewezen Certificatiedienstverleners (CSP's zijn: Digidentity, EAG, KPN en QuoVadis) een PKIO-certificaat worden aangevraagd.
[4] Indien de bewerker een private onderneming is, dan krijgt de bewerker een OIN toegewezen op basis van het KvK-nummer.

Sluit een geautoriseerde partij rechtstreeks aan op de BRP en beschikt deze nog niet over een PKIO-certificaat met eigen OIN, dan vraagt de geautoriseerde partij zelf zijn PKIO-certificaat en OIN aan.

In de BRP worden geen afzonderlijke certificaat-gegevens opgenomen. Nadat is vastgesteld dat het certificaat een geldig PKIO-certificaat is, gaat de voorgestelde oplossingsrichting er vanuit dat het in het certificaat opgenomen OIN vertrouwd kan worden en vanaf dat moment in het proces gebruikt wordt voor de identificatie van de betreffende partij in de verdere BRP-verwerking.

Indien een geautoriseerde partij zijn bewerker machtigt voor zowel de rol van transporteur als van ondertekenaar dan hoeft de geautoriseerde partij niet zelf een PKIO-certificaat en OIN aan te vragen ten behoeve van de communicatie met of de identificatie binnen de BRP. Dit moet zijn gemachtigde bewerker doen. Verzorgt een bewerker de communicatie met de BRP voor twee of meer geautoriseerde partijen, dan volstaat één PKIO-certificaat voor de rol van transporteur en één PKIO-certificaat voor de rol van ondertekenaar. Indien deze bewerker de TLS-afhandeling voor het versleuteld verzenden op dezelfde (proxy)server met dezelfde Certificate Name (CN) regelt, kan de bewerker hetzelfde PKIO-certificaat gebruiken voor ondertekening én versleuteld verzenden van berichten.

2.4 Authenticatie in de BRP

Met authenticatie wordt in de BRP geregeld dat altijd is te achterhalen welke juridisch geautoriseerde partij welke gegevens van wie heeft opgevraagd c.q. verstrekt heeft gekregen. Ook al heeft deze geautoriseerde partij voor de daadwerkelijke bevraging en levering een bewerker ingeschakeld.

Elke juridisch geautoriseerde partij krijgt een unieke partijcode. Om vast te kunnen stellen of deze geautoriseerde partij conform zijn autorisatie gegevens opvraagt/geleverd krijgt, is meer informatie nodig dan alleen de partijcode.

In de BRP wordt de autorisatie voor personen (doelgroep), gegevens en dienst(en) vastgelegd in een leveringsautorisatie. Elke huidige autorisatie van een afnemer wordt uitgewerkt naar één of meer leveringsautorisaties. Ook elke leveringsautorisatie krijgt een code toegekend.

Binnen het koppelvlak Leveren moet in elk bericht van/naar de BRP zowel de partijcode van de geautoriseerde partij als de code van de bijbehorende leveringsautorisatie zijn opgenomen.

Overigens krijgt ook elke bewerker bij registratie in de BRP een partijcode toegewezen. Deze partijcode van de bewerker zal echter nooit in een bericht van /naar de BRP opgenomen kunnen worden. Deze code is nodig om een bewerker als partij te kunnen registreren in de BRP.

2.5 Autorisatie in de BRP

Samengevat spelen de volgende gegevens een rol wat betreft de autorisatie in de BRP:

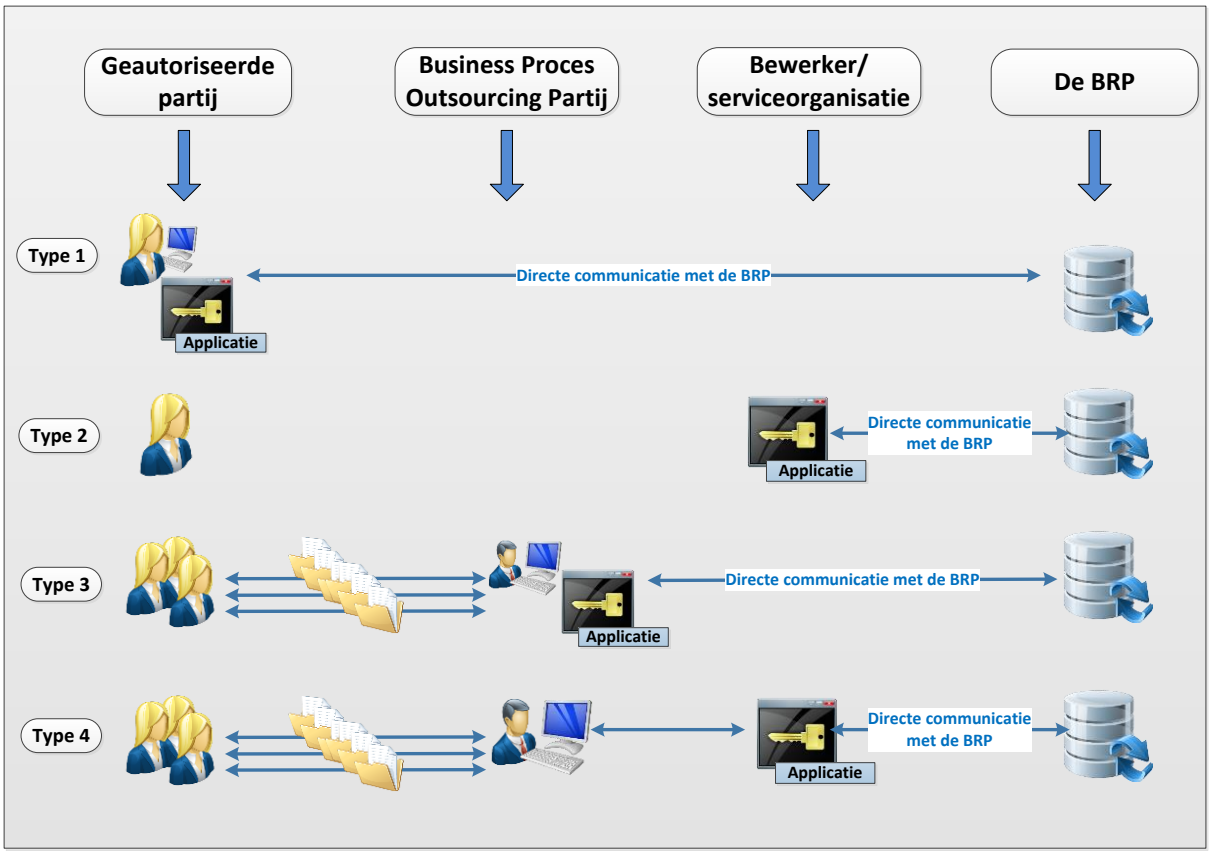
- De identiteit van de ondertekenaar; deze wordt door de BRP vastgesteld op basis van de OIN van de ondertekenaar;
- In geval van machtigingen controleert de BRP de geldigheid van deze machtiging(en);
- In elk bericht van en naar de BRP is de partijcode van de geautoriseerde partij en de code van de bijbehorende leveringsautorisatie opgenomen;

Indien een geautoriseerde partij voor de communicatie met de BRP een bewerker heeft gemachtigd, dient deze bewerker te beschikken over de partijcode en de code van de leveringsautorisatie van de geautoriseerde partij om in elk bericht aan de BRP op te kunnen nemen. De geautoriseerde partij blijft altijd *verantwoordelijk* voor het correct opnemen van de partijcode en code van de leveringsautorisatie in berichten, ook al heeft hij voor de uitvoering ervan zijn bewerker gemachtigd.

De geautoriseerde partij blijft in dat geval ook de eindverantwoordelijke voor de beveiliging van de gegevens bij bewerker(s), het transport tussen bewerkers en het transport tussen de geautoriseerde en een bewerker. De geautoriseerde partij kan deze eindverantwoordelijkheid niet contractueel verleggen naar een andere partij. Het wordt daarom sterk aanbevolen om de communicatie tussen de geautoriseerde partij en zijn bewerker op een zelfde beveiligde manier tot stand te laten komen als de communicatie tussen de BRP en de bewerker. Hierover maakt de geautoriseerde partij zelf afspraken met zijn bewerker.

3. Inrichting authenticatie per type aansluiting

De wijze waarop authenticatie per geautoriseerde partij geregeld moet worden, is afhankelijk van de manier waarop deze partij gaat aansluiten op de BRP. Er zijn in de basis vier verschillende typen aansluiting op de BRP mogelijk (zie onderstaand plaatje). Een toelichting op deze typen vindt u op de afnemerssite (http://www.operatiebrp.nl/vier-typen-aansluitingen).



Deze typen aansluiting gaan ervan uit dat één partij zowel de rol van Transporteur als Ondertekenaar vervult. In geval van type 1 is dit de geautoriseerde partij zelf. In geval van typen 2, 3 of 4 is dit de bewerker.

Zoals uitgewerkt in paragraaf 2.2 kan de geautoriseerde partij onderscheid maken naar uitvoering van de rol van Transporteur en de rol van Ondertekenaar. In onderstaande tabel zijn de mogelijkheden weergegeven:

Type aansluiting	Transporteur	Ondertekenaar
Rechtstreeks	Geautoriseerde partij	Geautoriseerde partij
Bewerker voor Transport	Bewerker	Geautoriseerde partij
Bewerker voor Ondertekening	Geautoriseerde partij	Bewerker
Eén bewerker voor Ondertekening en Transport	Bewerker 1	Bewerker 1
Verschillende bewerkers voor Ondertekening en Transport	Bewerker 1	Bewerker 2

Zoals uit de tabel blijkt, kan de rol van Transporteur of Ondertekenaar alleen bij een geautoriseerde partij of een bewerker belegd worden, nooit bij de BPO. In geval van type 3 is dezelfde organisatie weliswaar zowel BPO als bewerker. Maar alleen vanuit zijn rol als bewerker kan deze partij gemachtigd worden voor de rol van Transporteur en/of Ondertekenaar.