



Operatie BRP

Identificatie, authenticatie en
autorisatie in de BRP

Tanja Mundt

Coördinator Implementatie BRP
afnemers

Lilith Willemier Westra

Sasja van Immerzeel

Relatiebeheerders RvIG

Agenda

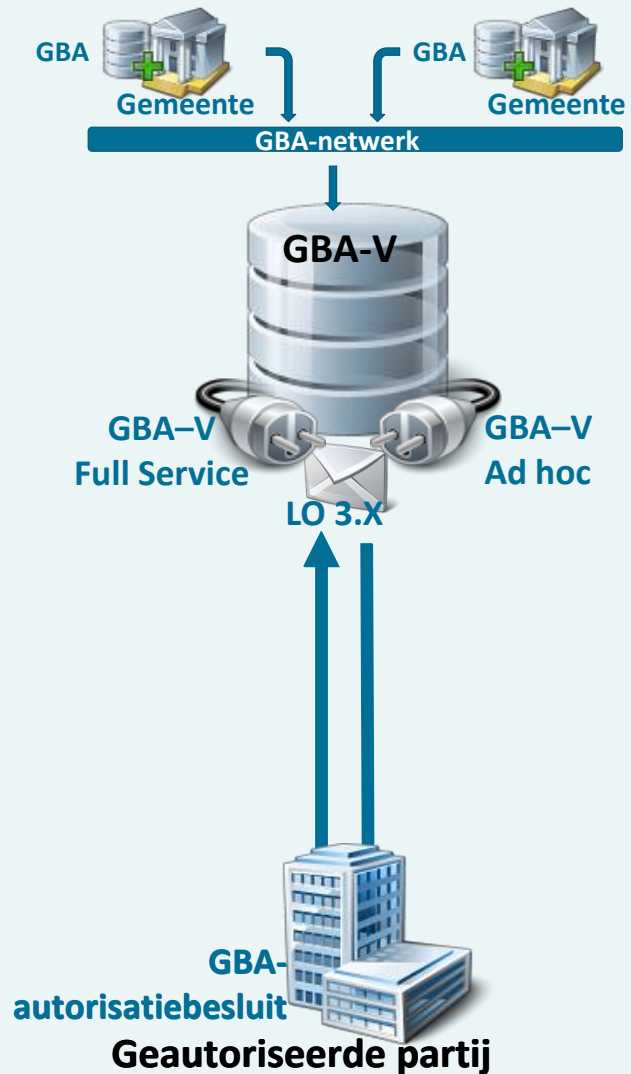
- Van GBA-V naar de BRP in vogelvlucht
- Type aansluitingen op de BRP
- Identificatie & authenticatie in de BRP
- Technische autorisatie
- De BRP Pub Quiz



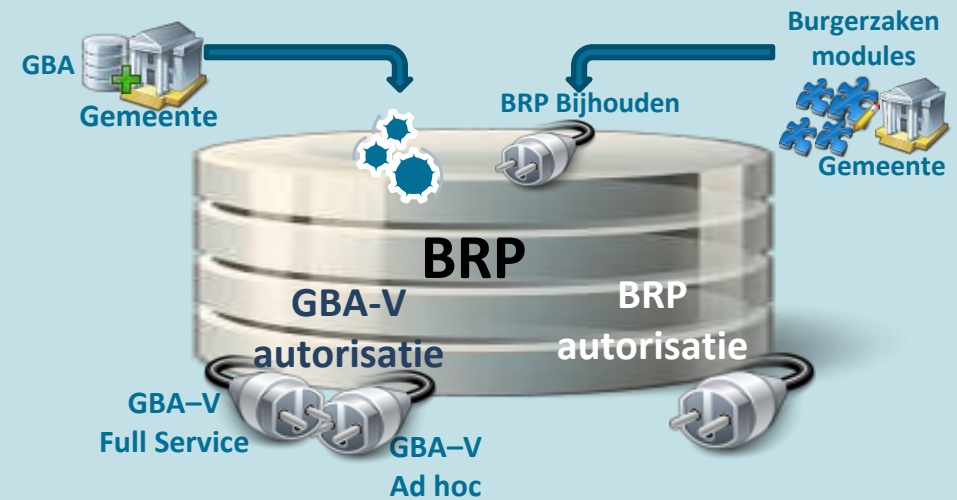
Van GBA-V naar de BRP in vogelvlucht



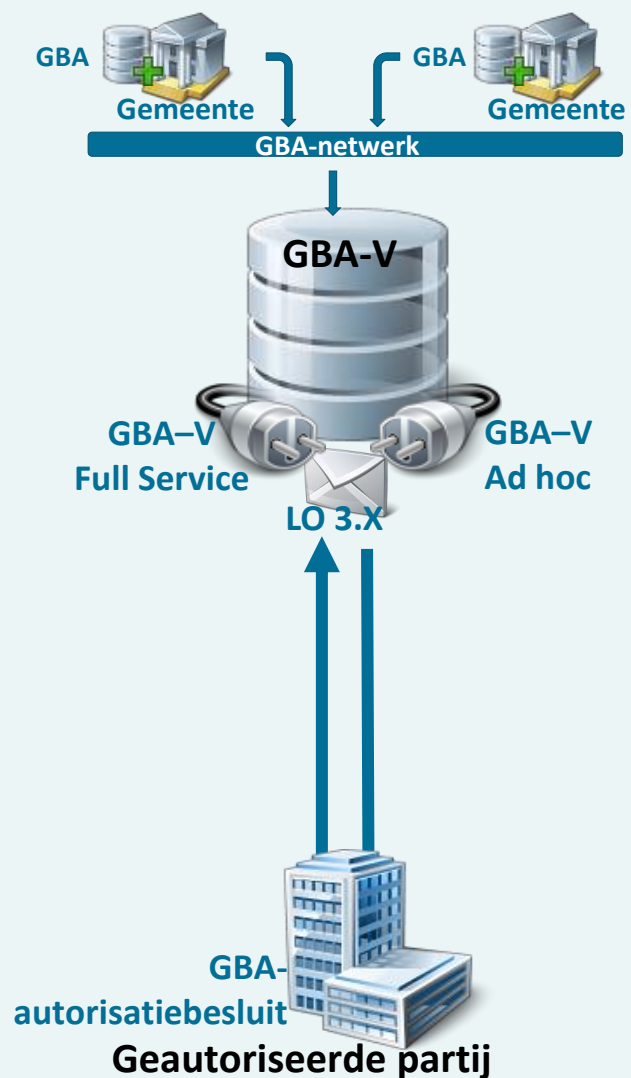
Huidige situatie GBA-V



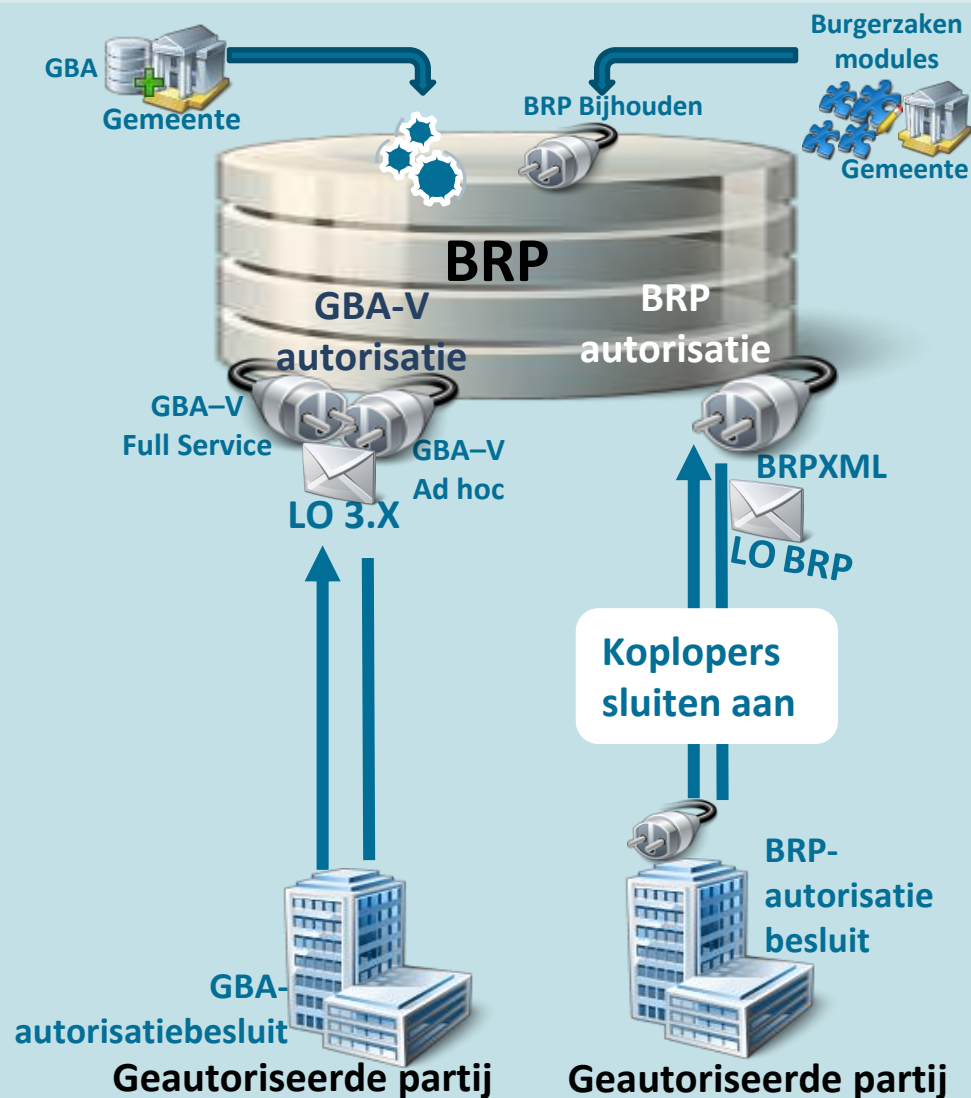
Ontwikkeling BRP

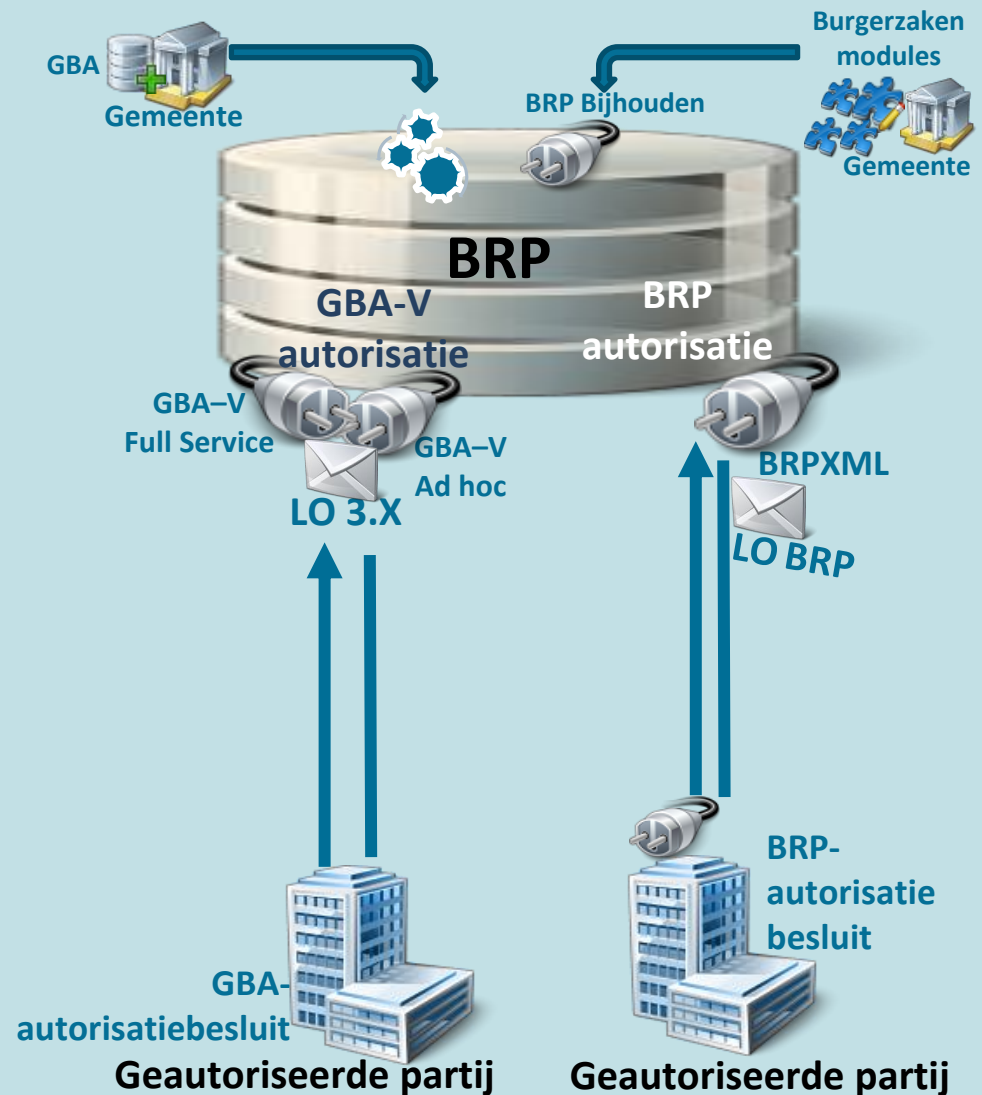


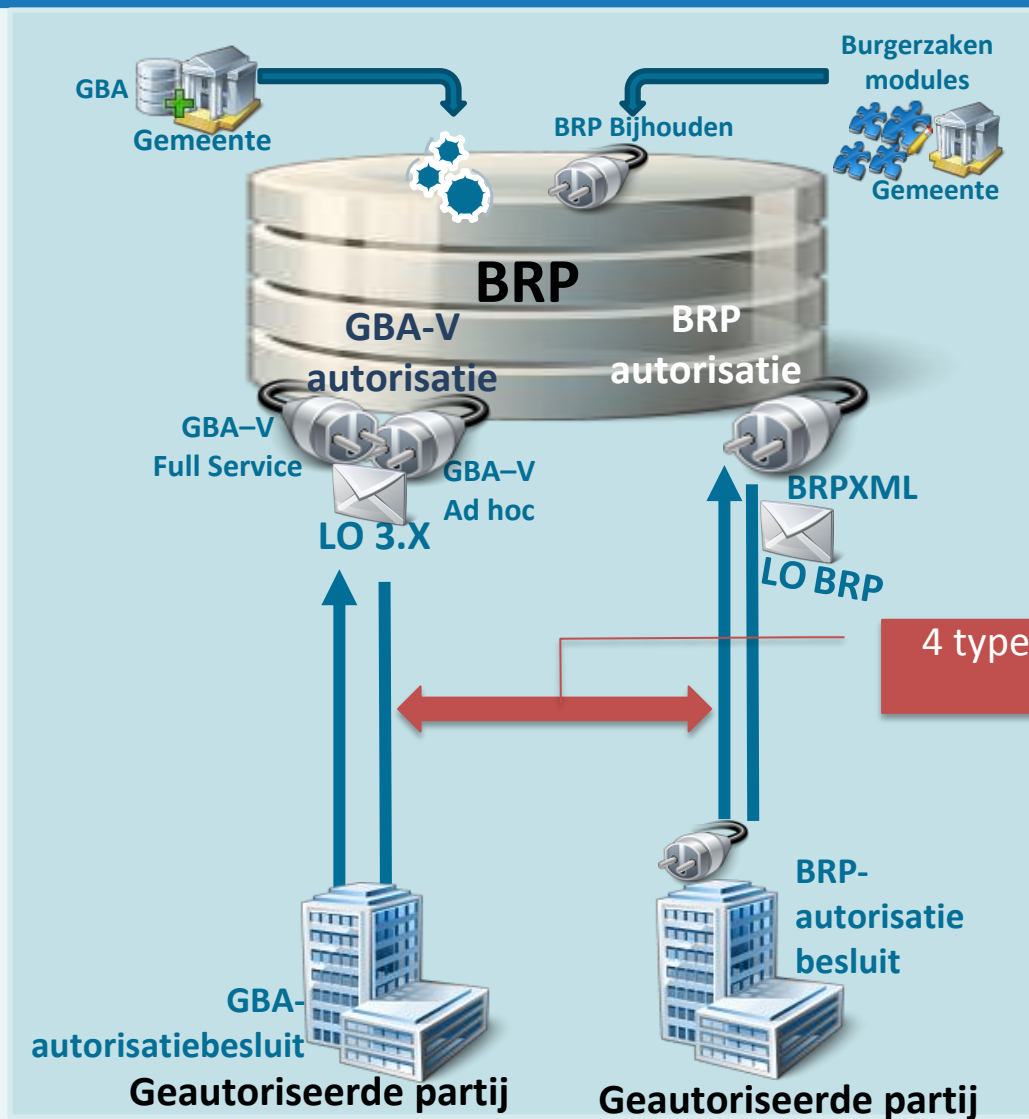
Huidige situatie GBA-V



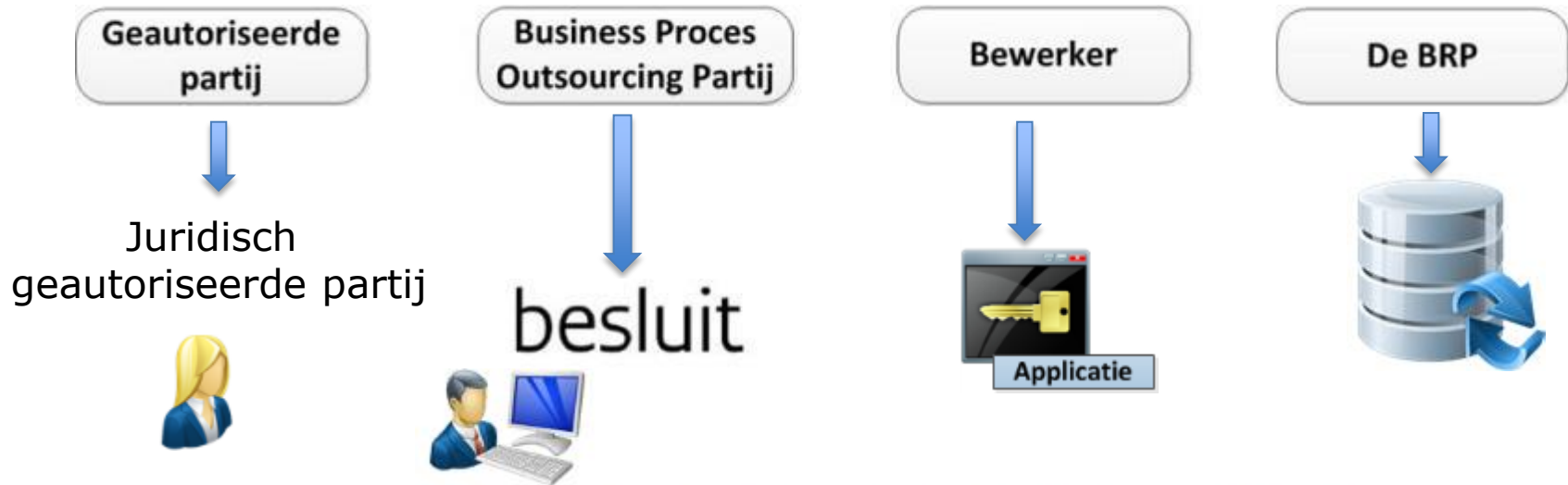
Start transitieperiode BRP







Aansluiten op de BRP: 4 rollen



In de verzoeken van 20 november 2014, 2014-0000632451 en van 29 december 2014, 2014-0000700195, heeft AZL N.V. namens de in bijlage I genoemde pensioenuitvoerders verzocht om autorisatie voor de systematische verstrekking van gegevens uit de basisregistratie personen in verband met de uitvoering van uitvoeringsovereenkomsten als bedoeld in artikel 1 van de Pensioenwet.

Gelet op de artikelen 3.1 en 3.3 van de Wet basisregistratie personen en artikel 39 van het Besluit basisregistratie personen wordt op dit verzoek als volgt besloten.

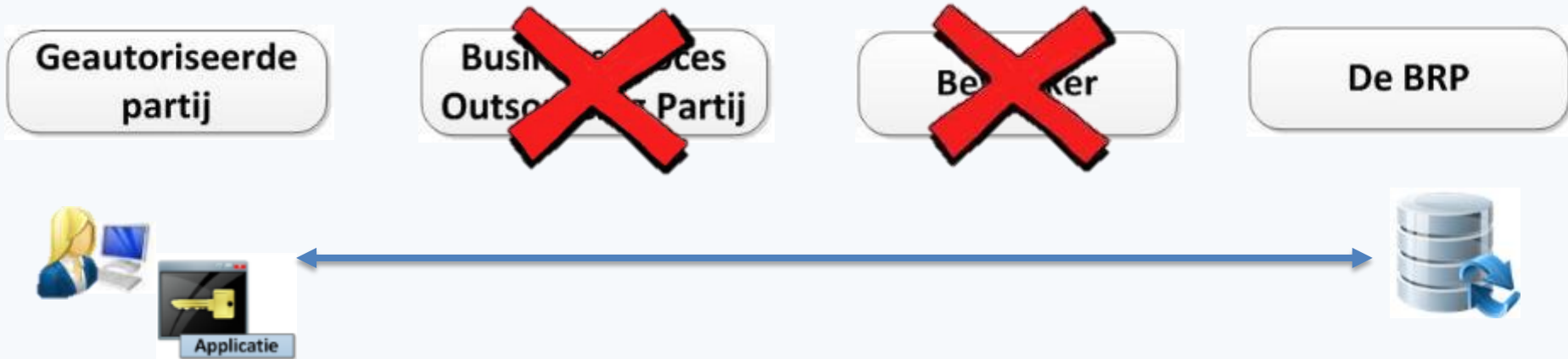
Paragraaf 1. Begripsbepalingen

Artikel 1

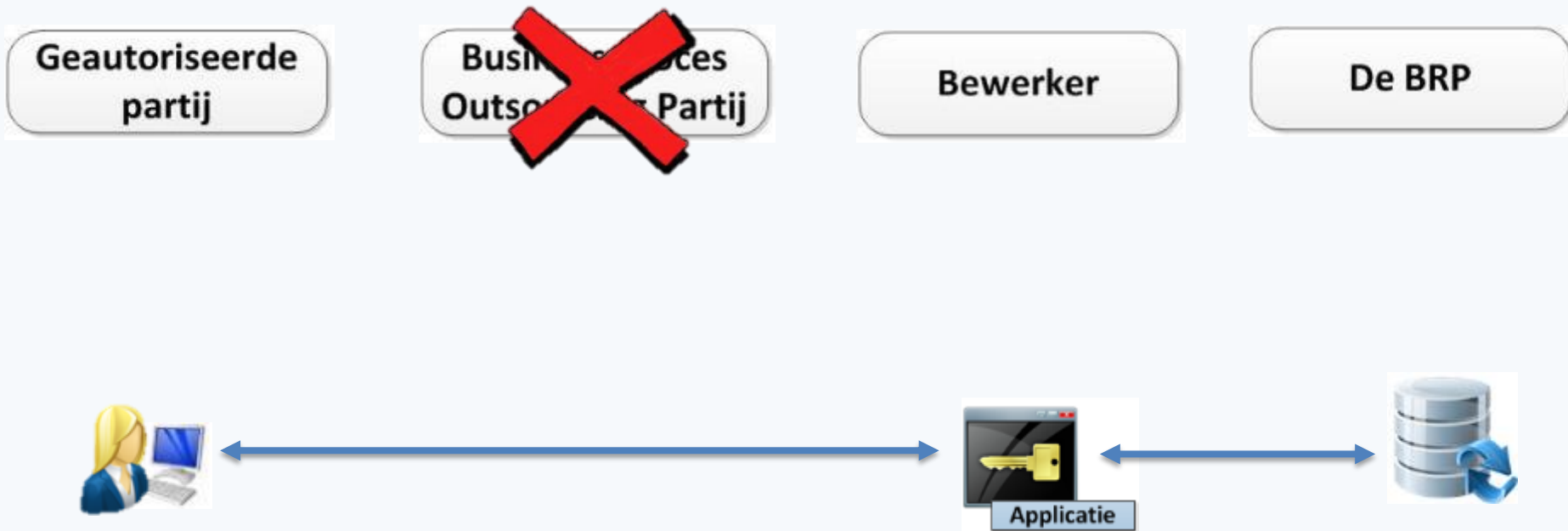
In dit besluit wordt verstaan onder:

- de pensioenuitvoerder: de in bijlage I genoemde pensioenuitvoerders;

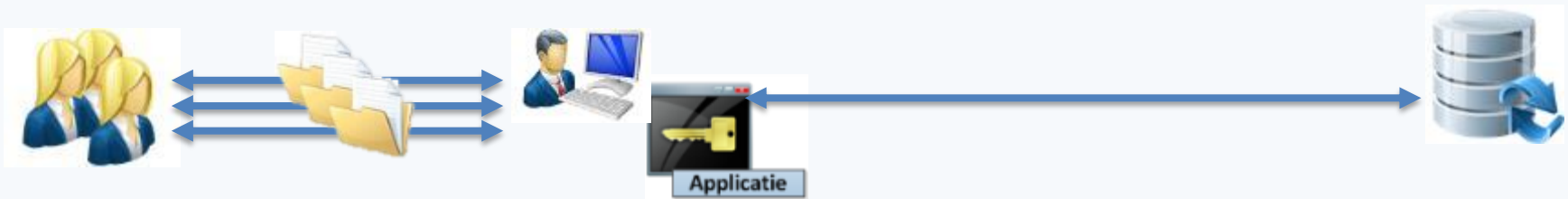
Type 1: geautoriseerde partij is zelf rechtstreeks aangesloten



Type 2: geautoriseerde partij sluit via bewerker aan



Type 3: geautoriseerde partij sluit via BPO = bewerker aan



Type 4: geautoriseerde partij sluit via BPO en bewerker aan



HOE BENT U NU AANGESLOTEN OP GBA-V?



**Geautoriseerde
partij**

**Business Proces
Outsourcing Partij**

Bewerker

De BRP



Uw type aansluiting op de BRP bepaalt voor de geautoriseerde partij:

- De mate waarin u werkzaamheden kunt uitbesteden in de voorbereiding om aan te kunnen sluiten op de BRP;
- Of juist alle voorbereiding zelf moet doen om aan te kunnen sluiten op de BRP;
- De wijze waarop u identificatie & authenticatie moet inrichten.



Identificatie & authenticatie in de BRP heeft betrekking op & stelt eisen aan:

- ✓ Communicatie met de BRP
- ✓ Identificatie van partijen in de BRP
- ✓ Authenticatie van de geautoriseerde partij in berichtuitwisseling met de BRP



Communicatie met de BRP



Communicatie met de BRP (1)

- Communicatie met BRP volgt Digikoppeling 3.0 standaard met PKIO-certificaat voor:
 - Versleuteling bericht t.b.v. transport (encryptie)
 - Elektronische ondertekening bericht (signing)
- In de berichtuitwisseling onderscheid naar:
 - Synchrone communicatie (bevraging)
 - Asynchrone communicatie (mutatielevering, selecties)
- Digikoppelingprofiel synchrone communicatie:
 - **2W-be-S** = WUS met 2-zijdige TLS + signing
- Digikoppelingprofiel asynchrone communicatie:
 - **2W-R-S** = WSRM (reliable messaging) + signing

(NB: over het gebruik van ebMS als protocol voor de BRP vindt nog overleg plaats)



Communicatie met de BRP (2)

- Geautoriseerde partij sluit aan op de BRP.
- Geautoriseerde partij kan voor het opzetten van de directe communicatie met de BRP gebruik maken van een bewerker.
- Geautoriseerde partij machtigt bewerker voor:
 - Rol van Transporteur;
 - Rol van Ondertekenaar;
 - 1 bewerker machtigen voor beide rollen? 1 PKIO-certificaat volstaat.
- Geautoriseerde partij geeft aan RvIG de machtiging(en) door.
- RvIG registreert machtigingen/gemachtigde partijen (met OIN) in de BRP.



Communicatie met de BRP (3)

- Vóór aansluiting op de BRP:
 - Uitwisselen IP-adressen met RvIG t.b.v. whitelist
 - Bij asynchrone communicatie: adres ontvangstsERVICE
- Bij rechtstreekse aansluiting:
 - Uitwisseling IP-adressen tussen geautoriseerde partij en RvIG.
- Bij machtiging bewerker:
 - Uitwisseling IP-adressen tussen bewerker en RvIG.
- Bij het opzetten van communicatie en verwerking van binnenkomende berichten valideert de BRP of:
 - PKIO-certificaat valide is;
 - Er geldige machtiging(en) aanwezig zijn.



Identificatie van Partijen in de BRP



Identificatie van partijen in de BRP

- Partij identificeert zich in de communicatie met de BRP met eigen PKIO-certificaat incl. unieke OIN.
- Identificatie bij rechtstreekse aansluiting:
 - Geautoriseerde partij identificeert zich met eigen PKIO-certificaat incl. unieke OIN
- Identificatie bij machtiging bewerker:
 - Bewerker identificeert zich met eigen PKIO-certificaat incl. unieke OIN
 - Bewerker = private partij: OIN o.b.v. KvK nummer
- Indien bewerker communicatie met de BRP verzorgt voor 2 of meer geautoriseerde partijen, dan volstaat een en hetzelfde PKIO-certificaat.



Authenticatie van de geautoriseerde partij in berichtuitwisseling met de BRP

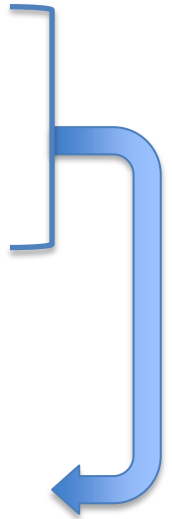


Uitgangspunt dat in juridische zin altijd te achterhalen is

- welke geautoriseerde partij,
- welke gegevens,
- van wie heeft opgevraagd c.q. verstrekt heeft gekregen.

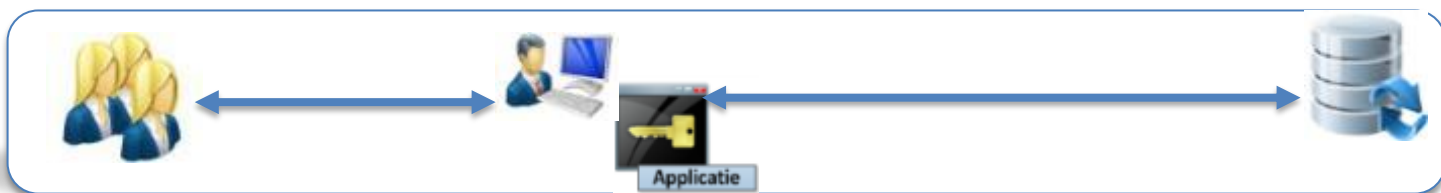
Stelt eisen aan:

- Inrichting BRP;
- Samenstelling berichten van/naar de BRP;
- Afspraken geautoriseerde partij, (BPO) en bewerker.



Inrichting van de BRP

- Registratie van partijen in de BRP:
 - Partijen zijn geautoriseerde partijen en bewerkers;
 - Een BPO wordt alleen *in de rol van bewerker* als partij geregistreerd (i.g.v. type 3 aansluiting);



- Een BPO wordt in het kader van authenticatie in de BRP niet als partij onderkend (type 3 en 4).



Inrichting van de BRP

- Vastleggen van abonnementen voor geautoriseerde partijen.
- Een abonnement legt de relatie tussen dienst en gegevens in autorisatiebesluit BRP.
- Registratie van machtigingen voor:
 - Transport;
 - Ondertekening + toegang abonnement.



Samenstelling van berichten

- Partijcode van de geautoriseerde partij opnemen in stuurgegevens van elk bericht van/naar de BRP.
- Abonnementnaam in parameters van elk bericht van/naar de BRP.
- Partijcode van de bewerker wordt alleen gebruikt voor identificatie in de BRP. Deze partijcode wordt nooit in de stuurgegevens van een bericht opgenomen.



Afspraken geautoriseerde partij, (BPO) en bewerker:

- Bewerker moet beschikken over Partijcode en abonnementnaam van geautoriseerde partij voor samenstellen van bericht.
- Geautoriseerde partij is eindverantwoordelijk voor correcte samenstelling bericht.
- Geautoriseerde partij is eindverantwoordelijk voor naleving:
 - Wbp (Wet bescherming persoonsgegevens)
 - Wet BRP (Wet basisregistratie personen)
- Uitvoering kan bij BPO belegd blijven.



Identificatie & authenticatie in de BRP

De verschillen tussen typen aansluiting



Identificatie & authenticatie in de BRP

Rechtstreekse communicatie (type 1)	Aansluiting via bewerker (type 2, 3, 4)
Geautoriseerde partij sluit aan op de BRP	Geautoriseerde partij sluit aan op de BRP
Geautoriseerde partij regelt zelf transport & ondertekening van berichten	Geautoriseerde partij machtigt bewerker voor transport/ondertekening van berichten/toegang tot abonnement
Geautoriseerde partij gebruikt eigen PKIO en OIN in communicatie met de BRP	Bewerker gebruikt eigen PKIO en OIN in communicatie met de BRP
Geautoriseerde partij is als enige partij geregistreerd voor aansluiting X	Geautoriseerde partij EN bewerker zijn beiden als partij geregistreerd voor aansluiting X
Uitwisseling IP-adressen tussen geautoriseerde partij en RvIG	Uitwisseling IP-adressen tussen bewerker en RvIG
Partijcode + abonnementnaam van geautoriseerde partij in bericht van/naar de BRP	Partijcode + abonnementnaam van geautoriseerde partij in bericht van/naar de BRP



Autorisatie in de BRP

- ✓ **Technische autorisatie**
- ✓ **Juridische autorisatie (plenaire sessie)**



Consequenties voor Bewerkersconstructies:

- Bewerkersconstructie is eigenlijk BPO-constructie;
- Nu in GBA-V: protocollering op naam BPO;
- Straks in de BRP: protocollering op partijcode geautoriseerde partij;
- BPO zal eigen systeem en processen moeten aanpassen;
- RvIG neemt contact op met de 'ingewikkelde constructies'.



Consequenties voor bestuursorganen:

- Autorisatiemodel BRP is anders dan huidig model.
- Het model biedt een brede marge: van globale autorisatie tot autorisatie in detail.
- RvIG i.s.m. oBRP richt zich op werkbaar model voor afnemer en beheerder.



De BRP Pub Quiz



De BRP Pub Quiz

Wie kan een **partijcode** krijgen in de BRP?

1. Juridisch geautoriseerde partij, BPO en Bewerker
2. Juridisch geautoriseerde partij en Bewerker
3. Alleen de juridisch geautoriseerde partij
4. BPO en Bewerker



De BRP Pub Quiz

Voor welke rollen kan je een Bewerker machtigen?

1. Vervoerder, Ondertekenaar, Toegang gegevens
2. Opsteller, Toegang doelbinding en Transporteur
3. Transporteur en Ondertekenaar
4. Transporteur, Ondertekenaar, Toegang abonnement



De BRP Pub Quiz

Welke uitspraak is waar?

1. Ad hoc bevraging is een voorbeeld van asynchrone communicatie
2. De partijcode van een bewerker kan bij hoge uitzondering opgenomen worden in een bericht
3. Een partij identificeert zich in de communicatie met de BRP met eigen PKIO-certificaat incl. unieke OIN
4. Alleen geautoriseerde partij en RvIG wisselen IP-adressen uit.





Stuur uw vraag naar:
implementatieteambrp@operatiebrp.nl

