Aspectbeschrijving – Autorisatiemodel

Versie 1.0

Datum 09 juni 2017

Status Definitief

Documenthistorie

Datum	Versie	Beschrijving	Auteur
07-06-2017	0.1	Initiele versie	Operatie BRP
08-06-2017	0.2	Na peer review	Operatie BRP
09-06-2017	1.0	Referentie opgenomen voor bijhouding	Operatie BRP

Reviewhistorie

Versie	Reviewer
0.1	Operatie BRP
0.2	Operatie BRP

Inhoudsopgave

1 Inleiding

1.1 Doel

In deze aspectbeschrijving wordt het autorisatiemodel van de centrale voorzieningen voor leveringsautorisaties uiteengezet.

1.2 Referenties

Nr.	Documentnaam	Organisatie	Versie	Datum
1	Leeswijzer BRP	Operatie BRP	-	-
2	Aspectbeschrijving Expressietaal	Operatie BRP	-	-
3	UCS BY.1.AA – Autorisatie administratieve handeling	Operatie BRP	-	-

2 Autorisatiemodel

2.1 Leveringsautorisatie

2.1.1 Achtergrond: 'privacy by design' en het aansluitproces

Het spreekt voor zich dat de overheid er aan gehouden is om zorgvuldig om te gaan met de persoonsgegevens in de basisregistratie personen. Deze plicht is ook nader vastgelegd in de Wet BRP en de Wet Bescherming Persoonsgegevens. Een centrale richtlijn is het 'privacy by design'. Dit gaat over:

1. 'privacy enhancing technologies' (beveiliging, encryptie);
2. dataminimalisatie: niet meer gegevens verwerken dan nodig is voor het beoogde doel.

Voor afnemers vertaalt het eerste element zich in technische aansluiteisen en het tweede element zich in het geleverd krijgen van een afgepaste set van gegevens die precies voldoende is voor het uitvoeren van de wettelijke of maatschappelijke taak waarvoor die afnemer de BRP nodig heeft. Omdat BRP afnemers heel diverse taken uitvoeren, moeten we die set voor elke afnemer afzonderlijk in kunnen richten. In het aansluitingsproces zal de stelselbeheerder samen met de afnemer vaststellen welke gegevens minimaal noodzakelijk zijn voor het uitvoeren van zijn de taak en via welke leveringsdiensten deze het handigste verstrekt kunnen worden. Dit proces leidt uiteindelijk tot een Leveringsautorisatiebesluit van de Minister voor die afnemer waarin beschreven staat welke diensten de afnemer mag afnemen en welke gegevens over welke personen daarbinnen geleverd worden. Aan de hand van dit leveringsautorisatiebesluit wordt de leveringsautorisatie in de BRP ingericht.

2.1.2 Autorisatie onderdelen

Dit onderwerp is onder te verdelen in de volgende onderdelen:

1. Partijautorisatie.

   Functioneel gaat dit om het vaststellen bij inkomende berichten dat we inderdaad met de partij te maken hebben aan wie een bepaalde autorisatie verleend is. In het geval van bewerkerconstructies heeft de geautoriseerde partij aangegeven dat één of meer andere partijen namens hem verzoeken digitaal mogen ondertekenen (proces outsourcing) of namens hem een beveiligde verbinding met de BRP mogen opzetten (technische outsourcing).

2. Dienstautorisatie.

   Hierbij gaat het er om dat we alleen die diensten aan afnemers verlenen waarop ze recht hebben. Bijvoorbeeld: als een afnemer die alleen personen mag bevragen verzoekt om een afnemerindicatie te plaatsen, dan zal het systeem dat weigeren.

3. Persoonsautorisatie.

   Hierbij gaat het er om dat we alleen gegevens aan de afnemer leveren over personen die hij nodig heeft voor zijn wettelijke of maatschappelijke taak. Als een afnemer bijvoorbeeld alleen gegevens nodig heeft van personen binnen zijn regio en een persoon bevraagt die buiten zijn regio woont, dan zal de BRP dit weigeren.

4. Gegevensautorisatie.

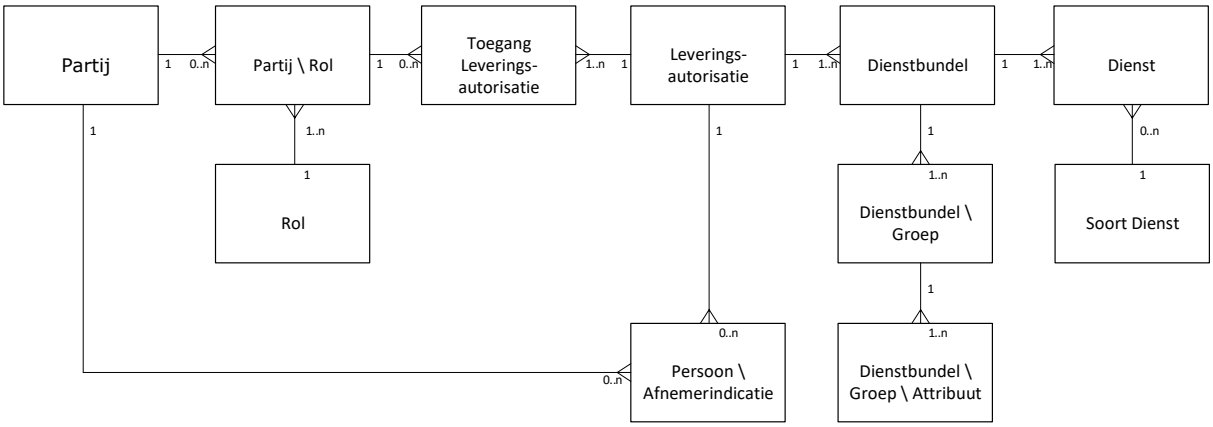
   Hierbij gaat het er om dat we van de personen die we leveren, alleen die gegevens leveren waar de afnemer recht op heeft. Als bijvoorbeeld de afnemer voor zijn proces geen gegevens nodig heeft over de ouders van de persoon en/of over zijn reisdocumenten, dan zullen die niet genoemd zijn in zijn autorisatiebesluit. De BRP zal die gegevens dan ook niet

leveren. Gegevensautorisatie valt nog uiteen in *attribuutautorisatie* en *aspectautorisatie* (mag de afnemer ook niet-actuele of vervallen gegevens ontvangen, en krijgt hij ook de nadere verantwoordingsgegevens te zien)

5. Modelautorisatie.

   Omdat er een aantal groepen van afnemers bestaan die hetzelfde autorisatieprofiel hebben (denk aan GGD'S, Waterschappen, Gemeenten, Notarissen, Gerechtsdeurwaarders) is het beheermatig handig om dezelfde autorisatie aan meer dan één partij toe te kunnen kennen. Dit noemen we een modelautorisatie.

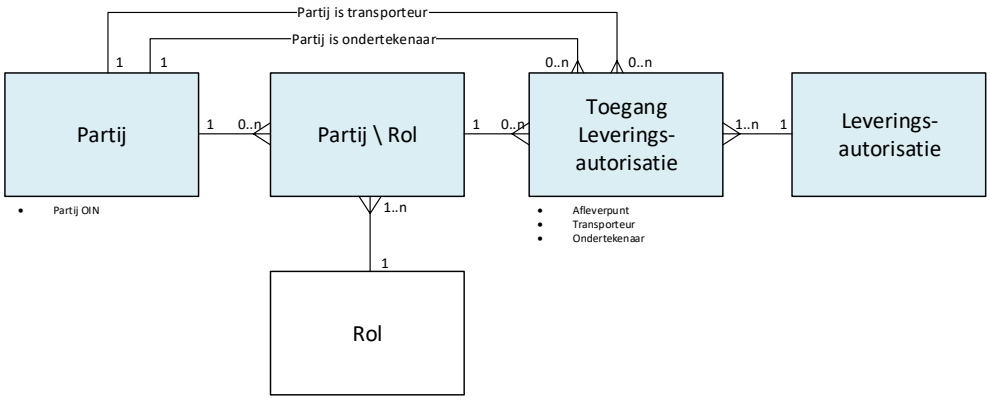
De inrichting van de bovenstaande onderdelen gebeurt in het AutAut schema van het BRP objectmodel (AutAut = Authenticatie en Autorisatie). Voor detailinformatie van dit schema kan het objectmodel worden geraadpleegd.



Figuur 1 Het AutAut schema

Het centrale objecttype is Leveringsautorisatie. De attributen van Leveringsautorisatie beschrijven in combinatie met de Dienstbundels en Diensten daarbinnen de volledige inrichting van een autorisatie. Via de Toegang Leveringsautorisatie wordt deze autorisatie vervolgens verstrekt aan één of meer Partijen, waarbij we ook de te gebruiken authenticatie en *'bewerkerconstructies'* vastleggen.

2.1.3 Partijautorisatie



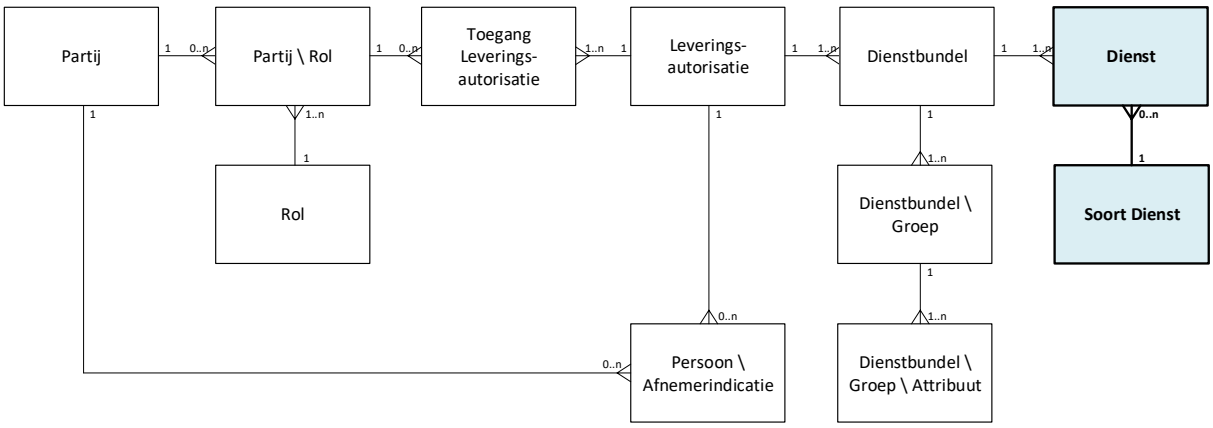
Figuur 2 Partijautorisatie

De authenticatie van inkomende berichten aan de BRP vindt plaats met behulp van PKI-overheidscertificaten. Dit resulteert uiteindelijk (als de certificaten geldig zijn gebleken) in een bericht met geverifieerde inhoud en twee OIN's: één van het certificaat dat gebruikt is voor de verbinding en één van het certificaat dat gebruikt is voor de digitale ondertekening. Met behulp van het OIN kan de BRP de partij terugvinden aan wie het certificaat behoort. Deze partij wordt aangeduid voor de verbinding als de 'transporteur'. Voor de ondertekening wordt deze partij de 'ondertekenaar' genoemd.

In het meest eenvoudige geval zijn de ondertekenaar en transporteur gelijk aan de partij die als afzender in het bericht wordt genoemd (de 'geautoriseerde partij'). Het is echter mogelijk dat deze partij anderen inschakelt om namens hemzelf een verbinding op te zetten of zelfs om namens hem digitaal te ondertekenen. Dit noemen we 'bewerkers'. De authenticatie in de BRP bestaat nu hieruit dat de combinatie van de geautoriseerde partij, transporteur en ondertekenaar in de BRP bekend moet zijn. Een bericht kan alleen via een kanaal worden aangeboden dat vooraf is aangemaakt en het bericht is ondertekend door een partij die hiervoor gemachtigd is. In alle andere situaties wordt communicatie dan wel berichtverwerking geweigerd.

Zoals in de bovenstaande afbeelding te zien is, wordt een partij altijd in combinatie met een bepaalde rol gekoppeld aan een autorisatie. Het zal echter niet zo zijn dat dezelfde partij met meerdere rollen aan dezelfde leveringsautorisatie wordt gekoppeld: een leveringsautorisatie voor een afnemersrol is principieel anders dan een leveringsautorisatie voor een bijhoudersrol. Voor één Leveringsautorisatie zullen dus alle Toegangen dezelfde Rol bevatten.

2.1.4 Dienstautorisatie



Figuur 3 Dienstautorisatie

Dienstautorisatie spitst zich toe op het objecttype Dienst. Bij verzoekberichten gaat het om de bepaling of de gevraagde Dienst geleverd mag worden. Daarnaast zijn er ook diensten die de BRP 'spontaan' levert, bijvoorbeeld naar aanleiding van een Administratieve Handeling waarover een afnemer geïnformeerd moet worden. De tabel Soort dienst is een enumeratie van de verschillende diensten die het systeem kan bieden, zoals het Plaatsen van een Afnemerindicatie. De Dienst is een unieke inrichting van die Soort dienst binnen een Leveringsautorisatie. Die ingerichte Dienst heeft een geldigheidsperiode en kan extra parameters bevatten, zoals het Attenderingscriterium voor een dienst van de soort Attendering of het Selectiecriterium voor een Selectie dienst.

2.1.4.1 Dienstautorisatie op verzoekberichten

In dit geval kan uit het verzoek worden vastgesteld welk voorkomen van Dienst gevraagd wordt. Voor dienstsoorten die maar één keer voor mogen komen binnen een Leveringsautorisatie is dit afleidbaar uit de opgegeven Leveringsautorisatie en de Soort bericht. Voor diensten die vaker voor mogen komen (zoals bevraging) moet de Dienst (via de identificatie) in het bericht expliciet

worden aangegeven. De dienstautorisatie bestaat dan uit de controle dat de betreffende Dienst inderdaad gevonden wordt en geldig is.

2.1.4.2 Dienstautorisatie bij spontane berichten

Er zijn ook diensten die niet worden getriggerd door een verzoek van de afnemer, maar door een administratieve handeling (Attendering, Mutatielevering) of die op een afgesproken tijdstip worden uitgevoerd (Selectie). Bij deze diensten verloopt de autorisatie dus anders: bij het opstarten van de betreffende service zal het systeem op zoek gaan naar diensten van de betreffende soort die op dat moment geldig zijn. Via de Toegang leveringsautorisatie kan dan vastgesteld worden hoe het resultaat bij de betreffende partij of partijen afgeleverd moet worden.

2.1.4.3 Meerdere dezelfde diensten, meerdere Leveringsautorisaties

In het algemeen geldt dat er van een dienst met een bepaalde Soort dienst, maar één voorkomen mag zijn onder een Leveringsautorisatie. De volgende Soorten diensten mogen echter meer dan één keer voorkomen in een autorisatie:

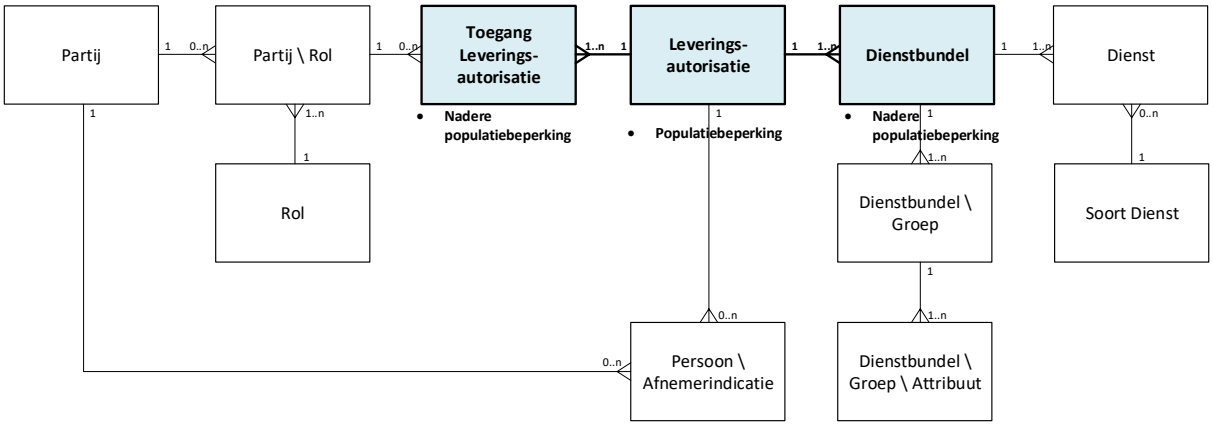
- Diensten die zoekfunctionaliteit bieden
- Bevragingsdiensten
- Selectiediensten

Dit betekent dat de afnemer bij een bevraging in het bericht aan moet geven welke specifieke dienst hij vraagt. Hiermee is het mogelijk om een afnemer meerdere bevragingsvarianten toe te kennen. Bijvoorbeeld een bevraging onder een dienstbundel met een kleine set van attributen waarmee alle ingeschrevenen mogen worden opgevraagd en een tweede bevraging met een grotere set van attributen voor een kleine doelgroep (en dus een striktere Nadere populatiebeperking voor die dienstenbundel).

Hiermee is het voor de meeste afnemers voldoende om één Leveringsautorisatie in te richten, met in het algemeen één tot drie dienstenbundels. In enkele gevallen zal het toch noodzakelijk zijn om afnemers meer dan één Leveringsautorisatie toe te kennen:

- Als een afnemer afnemerindicaties wil plaatsen bij verschillende populaties (en daar ook echt onderscheid in wil maken, bijvoorbeeld in de te verwerken set van gegevens). Een (fictief) voorbeeld daar van is het Openbaar Ministerie, dat zowel gegevens van justitiabelen als van slachtoffers verwerkt.
- Als een afnemer meerdere verschillende attenderingen wil ontvangen (die niet in één attendering gecombineerd kunnen worden). Dit komt alleen voor bij het CBS (tellingen van gebeurtenissen).
- Als een afnemer verschillende protocolleringsniveaus naast elkaar hanteert. Dit komt alleen voor bij de Politie en de inlichtingendiensten. Door op te geven welke leveringsautorisatie men gebruikt, bepaalt de afnemer ook het gehanteerde protocolleringsniveau.

2.1.5 Persoonsautorisatie



Figuur 4 Persoonsautorisatie

Een afnemer heeft vaak maar gegevens nodig van een deel van de personen uit de Nederlandse samenleving. Dikwijls kan de autorisatie beperkt worden tot personen uit een bepaalde regio of van een bepaalde leeftijdscategorie en geslacht. Veel afnemers hebben ook geen gegevens nodig van overleden personen. De BRP zal zoveel mogelijk voorkomen dat een afnemer gegevens van andere personen verwerkt dan hij voor zijn wettelijke of maatschappelijke taak nodig heeft. De BRP is echter niet in staat om dit volledig af te dwingen: een pensioenverzekeraar mag bijvoorbeeld slecht gegevens verwerken van zijn eigen verzekerden (en eventueel de partners en minderjarige kinderen van die verzekerden). De BRP kan echter op grond van de persoonslijst niet bepalen bij wie een persoon verzekerd is. Dus kan de BRP in dit geval niet voorkomen dat andere personen worden opgevraagd. De afnemer heeft hier echter zelf ook een verantwoordelijkheid in (die de stelselbeheerder bewaakt, bijvoorbeeld met audits en steekproeven).

Het controleren op de persoonsautorisatie gaat als volgt: De leveringsautorisatie heeft een Populatiebeperking. Dit is een attribuut dat een expressie kan bevatten (bijvoorbeeld de tekst: *geslachtsaanduiding = "M"*). Deze expressie wordt geëvalueerd over de kandidaat te leveren persoon. Dit levert drie mogelijke resultaten op:

- WAAR: de expressie is met zekerheid waar, en de persoon voldoet dus aan de gestelde populatiebeperking
- ONWAAR: de expressie is met zekerheid niet waar. De persoon voldoet niet aan de populatiebeperking en zal dus niet geleverd worden.
- NULL: het is niet eenduidig vast te stellen of de expressie al dan niet waar is (bijvoorbeeld omdat een bepaald gegeven niet aanwezig is of geheel of gedeeltelijk onbekend is). Ook in dat geval zal de persoon niet geleverd worden. Het is overigens wel mogelijk om de expressie zo vorm te geven dat deze ook bij het ontbreken/onbekend zijn van bepaalde gegevens het resultaat expliciet WAAR of ONWAAR oplevert.

Zie voor meer detail over expressies; Aspectbeschrijving Expressietaal **[2]**.

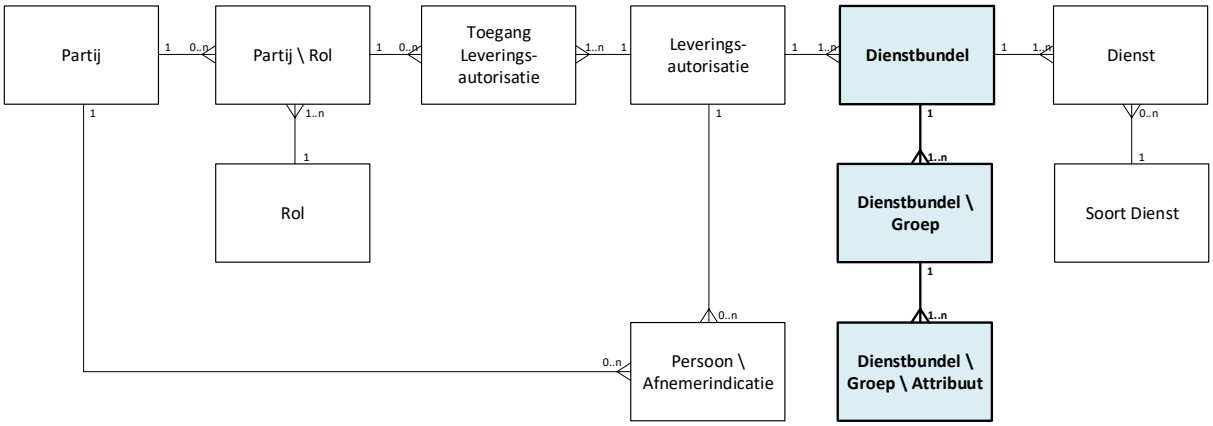
Naast de populatiebeperking in object Leveringsautorisatie zijn er ook Nadere populatiebeperkingen in Toegang leveringsautorisatie en Dienstbundel. Ook dit zijn expressies. De BRP gaat hier als volgt mee om: Bij het leveren van een bepaald bericht voor een bepaalde dienst zijn zowel de Toegang als de Leveringsautorisatie als de Dienst eenduidig bepaald. Het systeem maakt nu een totale expressie voor de populatiebeperking door deze drie componenten met een logische EN te verbinden. De uitkomst hiervan bepaalt uiteindelijk of de persoon geleverd wordt. Als één of meer van deze componenten geen waarde heeft, wordt deze beschouwd als WAAR.

De opsplitsing van deze expressie in drie componenten heeft het volgende doel:

- 'Leveringsautorisatie.Populatiebeperking' bevat de basale eis die voor alle diensten en voor alle afnemers minimaal geldt.
- 'Toegang leveringsautorisatie.Nadere populatiebeperking' bevat de eis die extra geldt voor deze toegang of voor de afnemer van deze toegang. Het meest voor de hand liggende gebruik van deze mogelijkheid is een extra regionale inperkingen bij verschillende regionale afnemers die gebruik maken van dezelfde modelautorisatie.

- ‘Dienstbundel.Nadere populatiebeperking’ kan een extra eis bevatten voor een dienstbundel die meer gegevens levert dan andere dienstbundels binnen dezelfde autorisatie. Stel bijvoorbeeld dat een specifieke bevraging gegevens over de ouders meelevert, maar dat die alleen bedoelt is voor het bevragen van minderjarige personen. De extra eis dat de leeftijd ten hoogste 18 jaar mag bedragen, wordt dan opgenomen in de nadere populatiebeperking van de dienstbundel van die bevraging.

2.1.6 Gegevensautorisatie



Figuur 5 Gegevensautorisatie

Welke gegevens over een persoon geleverd worden, leggen we vast per Dienstbundel. Een Dienstbundel is een clustering van een aantal diensten die logisch bij elkaar horen en juist daarom dezelfde set met gegevens leveren. Bijvoorbeeld: Als een afnemer in zijn eigen systeem een ‘lokale kopie’ van een persoon wil bijhouden, zal hij daarvoor de dienst Mutatielevering op afnemerindicatie afnemen die geconfigureerd is voor de set van gegevens die hij mag/wil verwerken. Maar voor hetzelfde doel zal hij ook de diensten Plaatsen afnemerindicatie, Verwijderen afnemerindicatie en Synchronisatie persoon moeten kunnen gebruiken, met allemaal diezelfde set van gegevens. Deze diensten vormen dan samen één Dienstbundel, waarbij we de set van te leveren gegevens maar één keer hoeven vast te leggen.

Voor elke gegevensgroep die een afnemer binnen zijn autorisatie (voor die bundel) mag verwerken wordt een voorkomen van Dienstbundel \ Groep aangemaakt. Hierin wordt de aspectautorisatie vastgelegd voor die betreffende groep:

- Mag de afnemer materiële historie (beëindigde gegevens) ontvangen van die groep?
- Mag de afnemer formele historie (vervallen gegevens) ontvangen van die groep?
- Mag de afnemer nadere verantwoordingsinformatie ontvangen van die groep?

Vervolgens moet ook worden aangegeven welke attributen van elke groep de afnemer mag ontvangen. Dit gebeurt door het aanmaken van voorkomens van Dienstbundel \ Groep \ Attribuut bij die groep.

Aandachtspunten:

- De autorisatie op groepen, aspecten en attributen betreft alleen de primaire gegevens op de persoonslijst. Ten aanzien van de groepen en attributen van nadere verantwoordingsgegevens en onderzoeksgegevens gelden afwijkende regels: als een afnemer recht heeft op nadere verantwoording bij een bepaalde groep, dan mag hij alle groepen van die verantwoording en alle te leveren attributen van die verantwoording ook geleverd krijgen. Ook bij onderzoek geldt dat als er een onderzoek bestaat bij een gegeven waarvoor hij geautoriseerd is, hij alle groepen en te leveren attributen van dat onderzoek zal ontvangen.

- Als de afnemer geen materiële historie mag zien, dan mag hij in principe ook de attributen met een materieel aspect niet hebben: Datum ingang geldigheid en Datum einde geldigheid. Echter: Datum ingang geldigheid behandelen we als een regulier attribuut omdat het regelmatig voorkomt dat een afnemer die alleen de actuele gegevens mag hebben toch dient te weten sinds wanneer die gegevens actueel zijn. Datum einde geldigheid zal nooit aanwezig zijn bij actuele gegevens. Kortom in de praktijk heeft deze filtering geen zichtbaar effect.
- Als een afnemer geen formele historie mag zien, dan mag hij ook de attributen met een formeel aspect niet zien: Tijdstip registratie en Tijdstip verval.
- Hoewel de autorisatie op formele historie per groep toegekend kan worden, is het bij relaties / gerelateerden logisch om dit voor de relatiestructuur als geheel al dan niet toe te kennen. Als de autorisatie anders wordt toegekend dan kunnen vreemde (lastig te interpreteren) berichten ontstaan. Bijvoorbeeld doordat de vervallen relatie wel maar de vervallen gerelateerden niet mogen worden getoond, is het niet meer duidelijk over welke relatie het gaat.
- In een mutatiebericht worden wel de groepen opgenomen die in de betreffende handeling vervallen zijn geraakt (als onderdeel van de 'delta'), ook voor afnemers die geen formele historie mogen zien.
- We spreken over 'nadere verantwoording' omdat afnemers standaard de omschrijving van de soort administratieve handelingen meegeleverd krijgen die zijn doorgevoerd bij de persoon. Echter: als de afnemer een beperkte autorisatie heeft geeft dit soms meer privacygevoelige informatie prijs dan wenselijk is. Zo hoeft een afnemer die alleen NAW gegevens krijgt niet te weten dat de reden dat de naam wijzigt: 'Adoptie' is. In dat geval kan in de Leveringsautorisatie worden opgenomen dat een Alias wordt geleverd die minder prijsgeeft over de achterliggende bijhouding. In dit geval zou dat bijvoorbeeld 'Afstamming' kunnen zijn.

Voor elk potentieel te leveren attribuut is een voorkomen aanwezig in de elementtabel. In dit voorkomen bevat Element.Autorisatie informatie over de autoriseerbaarheid van het attribuut, wat van belang is voor de invulling van de attribuutautorisatie. De volgende waardes zijn mogelijk:

- 'Via groepsautorisatie': dit zijn attributen waarvan de aspectautorisatie van de groep bepaalt of ze in het bericht worden opgenomen. Het gaat om attributen als Datum einde geldigheid (via materiële historie), Tijdstip registratie (via formele historie), Actie inhoud (via naderen verantwoording). Deze attributen dienen dus *niet* voor te komen in Dienstbundel \ Groep \ Attribuut.
- 'Niet verstrekken': dit zijn attributen die niet verstrekt mogen worden volgende de Wet BRP. Het gaat vooral om gegevens die zijn toegevoegd om de correcte werking van het systeem te faciliteren. Mogelijk kunnen ze via andere wetgeving nog wel verstrekt worden (zoals de Wet op de Inlichtingdiensten). Een voorbeeld is Persoon.Afgeleidadministratief.Sorteervolgorde, dat alleen gebruikt wordt om personen in een logische volgorde in een bericht te kunnen plaatsen (eerst de hoofdpersoon van een handeling, daarna pas de geraakte nevenpersonen).
- 'Optioneel': dit zijn de reguliere attributen waarbij per Dienstbundel (aan de hand van het leveringsautorisatiebesluit) bepaald kan worden of deze daar opgenomen dient te worden.
- 'Structuur': dit zijn attributen die impliciet geleverd worden via de structuur van het bericht, zoals foreign keys tussen objecten. Deze worden niet opgenomen in Dienstbundel \ Groep \ Attribuut.
- 'Verplicht': dit zijn attributen die volgens de wet (o.a. art. 3.10 Wet BRP) altijd geleverd moeten worden. Deze zijn daarom bij elke Dienstbundel opgenomen in Dienstbundel \ Groep \ Attribuut. (Bijvoorbeeld: Persoon.Bijhouding.BijhoudingsaardCode)
- 'Aanbevolen': dit zijn attributen waarbij geen wettelijke verplichting bestaat maar die normaliter altijd geautoriseerd zal worden. De beheerder kan hier echt afwijken. Ze zullen dus normaliter voorkomen in Dienstbundel \ Groep \ Attribuut. Voorbeeld is het Burgerservicenummer.
- 'Bijhoudingsgegevens': worden alleen vastgelegd ten behoeve van het bijhoudingsproces. Deze kunnen alleen worden geautoriseerd aan een afnemer met een bijhoudersrol. Een voorbeeld is Persoon.SamengesteldeNaam.IndicatieAfgeleid.

- 'Uitzondering': Voor deze attributen bestaat er een bedrijfsregel die bepaalt of deze in een bericht wordt opgenomen. Bijvoorbeeld de 'Indicatie aangetroffen op adres'. Deze wordt altijd geleverd (het is een soort van onderzoeksgegeven), maar alleen wanneer er enig adresgegeven geleverd wordt. Deze worden niet opgenomen in Dienstbundel \ Groep \ Attribuut.

2.1.7 Leveren aan bijhouders

Het is mogelijk om een Partij met een bijhoudersrol (Bijhouder College of Bijhouder Minister) toegang te geven tot een leveringsautorisatie. Hiermee kan bijvoorbeeld de dienst 'Geef details persoon' ook gebruikt worden in het kader van 'bevragen voor bijhouding'. Indien een leveringsdienst wordt aangeroepen met een bijhoudersrol, moet deze zich op een aantal punten anders gedragen wat doorwerkt in het autorisatiemodel:

- Bijhouders hebben recht op alle autoriseerbare gegevens, inclusief de 'bijhoudersgegevens' die niet autoriseerbaar zijn voor afnemers. Dit implementeren we door enerzijds alle autoriseerbare attributen expliciet op te nemen in Dienstbundel \ Groep \ Attribuut en anderzijds het wegfilteren van bijhoudersgegevens (met name uit de nadere verantwoording en de onderzoeksgegevens) niet uit te voeren als er sprake is van een bijhoudersrol. Deze oplossing is gekozen voor maximale toekomstige flexibiliteit (bijvoorbeeld als afwijkende bijhoudersprofielen nodig blijken voor bijvoorbeeld de IND of voor ABO's)
- Hetzelfde geldt ten aanzien van aspectautorisatie: bijhouders hebben altijd recht op alle materiële en formele historie en de nadere verantwoordingsinformatie. Dit richten we expliciet in door voor alle groepen een Dienstbundel \ Groep op te nemen en alle aspecten daar in te autoriseren.

2.1.8 Modelautorisaties

Er zijn een aantal wettelijke/maatschappelijke taken waarvoor BRP gegevens worden geleverd, die bij meer dan één partij zijn belegd. Meestal is daarbij sprake van een regionale onderverdeling die soms heel strikt is (bijvoorbeeld gemeenten, waterschappen, provincies) en soms niet of minder nauwkeurig is afgebakend (bijvoorbeeld GGD's, ziekenhuizen, notarissen, gerechtsdeurwaarders, pensioenverzekeraars). In deze situatie geldt dat afnemers van dezelfde soort ofwel een volledige identieke autorisatie zullen hebben (soms delen ze ook hetzelfde autorisatiebesluit) ofwel een autorisatie zullen hebben die alleen afwijkt qua regionale afbakening van de persoonsautorisatie.

Om het beheer op dit soort autorisaties enigszins eenvoudiger te maken, is het mogelijk gemaakt om modelautorisaties aan te maken en die toe te kennen (door het aanmaken van een Leveringsautorisatie) aan meerdere afnemers. Modelautorisaties zijn te herkennen aan Leveringsautorisatie.Modelautorisatie? = 'Ja' en de aanwezigheid van meerdere gerelateerde Toegang Leveringsautorisaties. Als er sprake is van een regionale afbakening dan wordt deze vastgelegd in Toegang leveringsautorisatie.Nadere populatiebeperking. De beperking die alle afnemers gemeenschappelijk hebben staat dan in Leveringsautorisatie.Populatiebeperking.

2.1.9 Blokkeren van autorisaties

De stelselbeheerder kan een leveringsautorisatie of een deel daarvan tijdelijk blokkeren, bijvoorbeeld als er aanwijzingen zijn voor misbruik of als een afnemer aangeeft tijdelijke problemen met de verwerking te hebben. Blokkeren is mogelijk op de volgende niveaus:

- Leveringsautorisatie: Het blokkeren van een Leveringsautorisatie treft alle diensten onder deze autorisatie voor alle afnemers die toegang hebben tot deze autorisatie. Zou de beheerder bijvoorbeeld de (model) leveringsautorisatie voor gerechtsdeurwaarders blokkeren, dan kan geen enkele gerechtsdeurwaarder nog enige dienst benaderen.
- Toegang leveringsautorisatie: Deze blokkeert alleen de specifieke toegang. Hiermee is het mogelijk om (bij een modelautorisatie) alleen een bepaalde afnemer te blokkeren of om

een toegang via een specifieke bewerker te blokkeren. De andere afnemers of toegangen die niet via deze bewerker lopen worden hierdoor niet geraakt.
- Dienstbundel: Deze blokkeert alle diensten onder deze bundel. Hiermee kunnen bijvoorbeeld alle diensten voor mutatielevering worden geblokkeerd, terwijl bevraging (aangenomen dat dit een aparte bundel is) wel mogelijk blijft. Als het een modelautorisatie betreft, geldt dit voor alle afnemers die deze gebruiken.
- Dienst: Dit blokkeert alleen de specifieke dienst. Als het een modelautorisatie betreft, geldt dit voor alle afnemers die deze gebruiken.

De gevolgen van een blokkering zijn als volgt:

- Een verzoekbericht voor een geblokkeerde dienst resulteert in een foutmelding, en de dienst wordt niet geleverd.
- Een dienst die berichten levert op grond van een handeling in het systeem (bijvoorbeeld Mutatielevering en Attendering) zullen geen berichten leveren.
- Selecties zullen niet worden gestart wanneer er sprake is van een blokkering.

Vooral het tweede punt heeft impact voor een afnemer: hij kan triggers missen voor zijn bedrijfsproces en zijn lokale persoonsgegevens zijn niet meer synchroon. Dit zal het noodzakelijk maken om naderhand reparatiewerkzaamheden uit te voeren. De beheerder moet dus weloverwogen gebruik maken van de mogelijkheid tot het blokkeren van diensten, vooral als het attendering en synchronisatie betreft.

2.1.10 Beperking op het inlezen van leveringsautorisatiegegevens

Autorisatiegegevens worden lang bewaard, onder andere omdat ze nodig zijn bij het vervaardigen van protocolleringsoverzichten. Dit betekent dus dat er veel meer historische autorisatiegegevens aanwezig zijn dat actuele autorisatiegegevens. Om onnodig impact op performance te voorkomen worden niet alle historische autorisatiegegevens ingeladen in het systeem: alle gegevens die langer dan drie maanden geleden zijn beëindigd, worden genegeerd. Voor de afnemende systemen betekent dit dat wanneer een autorisatie gebruikt wordt die beëindigd is, de eerste drie maanden de foutmeldingen zullen melden dat de betreffende autorisatie niet geldig is. Na die drie maanden zal het systeem melden dat de betreffende autorisatie niet bestaat.

2.2 Bijhoudingsautorisatie

Voor het autorisatiemode van de centrale voorzieningen voor bijhoudingsautorisaties zie UCS BY.1.AA – Autorisatie administratieve handeling **[3]**.