Functioneel Ontwerp IAM-systeem

Ten behoeve van

gemeente Zaanstad

ZNSTD

Kenmerk: 2026-198
Datum: 2-11-2026
Versie: Definitief 2.0.1

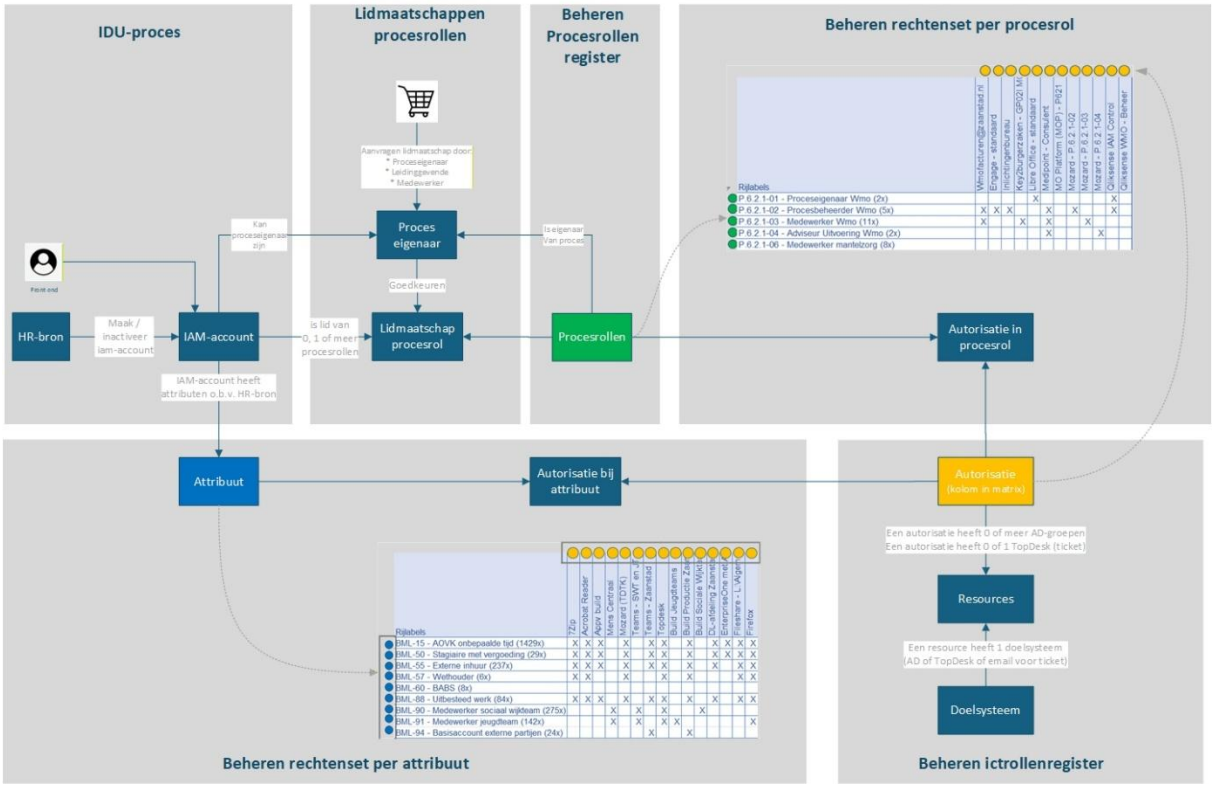
Inhoud

1 Inleiding 2
2 IDU-proces 3
2.1 Bronsystemen 4
2.2 Koppelen aan YouForce voor Zaanstad 4
2.3 Integrale IDU-keten 5
2.4 Bepalen HR-attributen 8
2.5 Overrulen HR-koppeling 9
2.6 Signalering doorstroom 9
3 Aanvragen en goedkeuren losse autorisaties en procesrollen 10
4 IAM-beheer 11
4.1 Beheren ICT-rollenregister 11
4.2 Functionaliteit ICT-rollenregister 11
4.3 Definities ICT-rollenregister 12
4.4 Definities vertaald naar voorbeeld 13
4.5 Gelaagde autorisatiestructuur – uitwerking voorbeeld 15
4.6 Beheren procesrollen 16
4.7 Beheren procesrolmatrices en attribuutmatrices 17
5 Conversie 19
Bijlagen 21
Bijlage 1 IAM-persoonskaarten 21
Bijlage 2 Identiteitscontainers 22
Bijlage 3 Koppeling AD 23
Bijlage 4 Koppeling YouForce 25
Bijlage 5 Koppeling TOPdesk 27

1 Inleiding

Hieronder een schematische weergave van het beoogde IAM-systeem verdeeld in 6 onderdelen. Elk onderdeel wordt functioneel beschreven.

Dit Functioneel Ontwerp beschrijft de vereiste functionele werking, samenhang en beheerresultaten. De opgenomen technische uitwerkingen, gegevensvelden, schema's en voorbeelden beschrijven de huidige situatie of een mogelijke realisatie. Een technisch afwijkende standaardinrichting is toegestaan, mits daarmee aantoonbaar dezelfde functionele werking, autorisatiestructuur, procesrollenstructuur, governance, traceerbaarheid en beheerbaarheid worden gerealiseerd. Een fundamentele aanpassing of herinrichting van de bestaande autorisatiestructuur, procesrollenstructuur of governance is niet gewenst.



Figuur 1 integraal overzicht IAM

2 IDU-proces

Zaanstad voert het instroom-, doorstroom- en uitstroomproces uit voor meerdere identiteitscontainers. Een identiteitscontainer is de organisatorische context waarin een identiteit wordt geregistreerd en beheerd. Een identiteitscontainer correspondeert met een organisatie of een nader te bepalen groep partnerorganisaties (zie ook bijlage 2 in dit document).

De definitieve indeling van de identiteitscontainers en de verdeling van de partnerorganisaties daarbinnen wordt tijdens de implementatie in overleg met Opdrachtnemer vastgesteld. Dit betreft een nadere concretisering binnen de beschreven scope en geen uitbreiding daarvan.

Voor de inrichting geldt het volgende indicatieve uitgangspunt:

- één identiteitscontainer voor Gemeente Zaanstad;
- één identiteitscontainer voor Stichting Jeugdteam;
- één identiteitscontainer voor Sociaal Wijkteam;
- één gezamenlijke identiteitscontainer voor de overige partnerorganisaties.

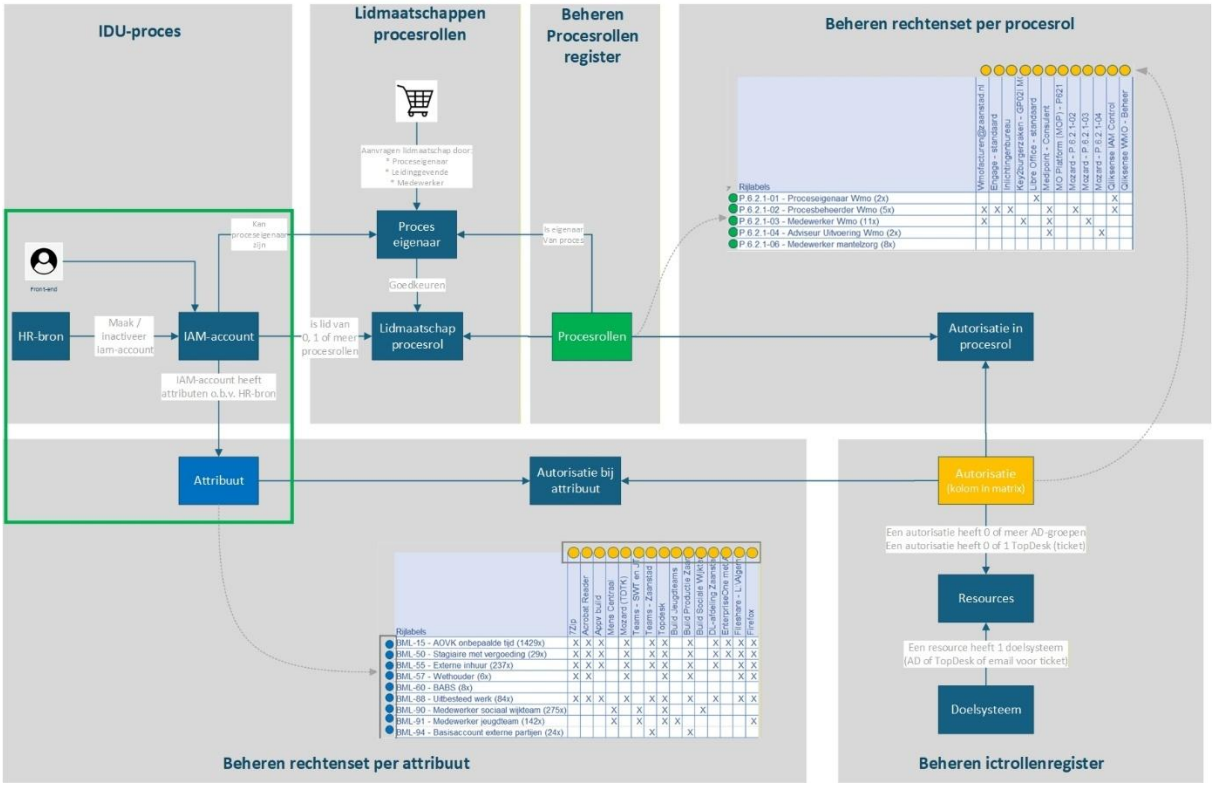
Tot de overige partnerorganisaties behoren momenteel onder andere Omgevingsdienst, Gemeente Oostzaan, Gemeente Wormerland en Pact Zaandam Oost. De Oplossing moet de mogelijkheid bieden om identiteitscontainers flexibel en beheersbaar in te richten en te beheren.

Voor Gemeente Zaanstad worden identiteiten vanuit YouForce verwerkt. Identiteiten van partnerorganisaties worden handmatig in de Oplossing ingevoerd.

De verschillende identiteitscontainers maken het mogelijk identiteiten en autorisaties per organisatorische context gescheiden te beheren. Een natuurlijke persoon kan gelijktijdig meerdere identiteiten in verschillende identiteitscontainers hebben. Iedere identiteit heeft een eigen IAM-persoonskaart en een eigen lifecycle. Naar verwachting komt dit bij minder dan twintig personen gelijktijdig voor. Het betreft veelal een tijdelijke situatie bij doorstroom van de ene organisatie naar een andere organisatie.

Voor de omvang van de Oplossing geldt als uitgangspunt circa 3.000 actieve identiteiten, met een bandbreedte van circa 20% meer of minder. De aantallen per organisatie of partnerorganisatie zijn indicatief. Een inactieve identiteit heeft geen actieve relatie, toegang of autorisatie meer en wordt uitsluitend bewaard voor audit, historie, bewaartermijnen of een eventuele herindiensttreding.

2.1 Bronsystemen



Figuur 2 Scope gekoppelde bronsystemen aan IAM

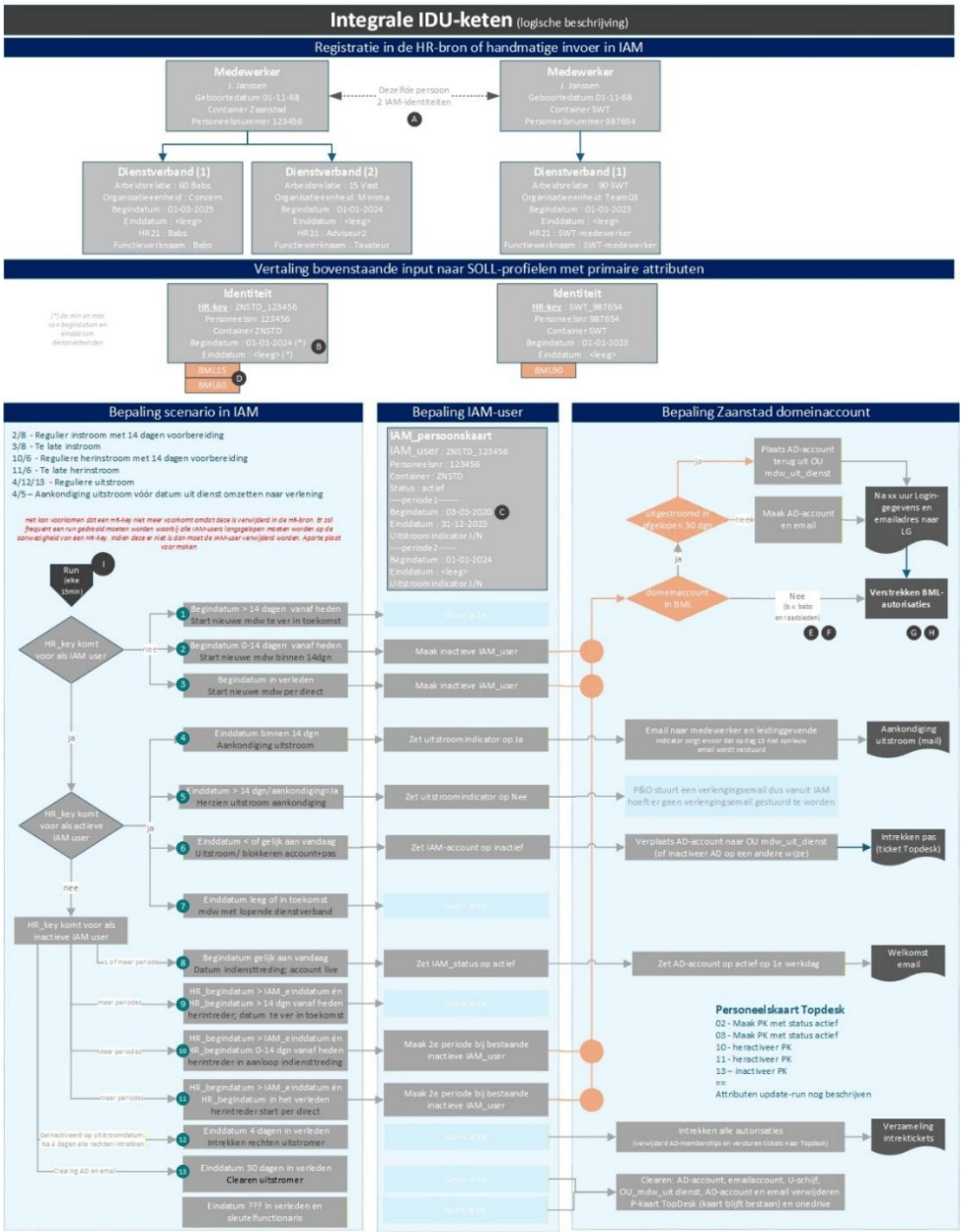
Voor Gemeente Zaanstad wordt één HR-systeem als bronsysteem aangesloten, namelijk YouForce. Identiteiten van partnerorganisaties worden handmatig rechtstreeks in de Oplossing ingevoerd. Voor beide invoerkanalen moet vervolgens dezelfde integrale IDU-keten kunnen worden toegepast.

2.2 Koppelen aan YouForce voor Zaanstad

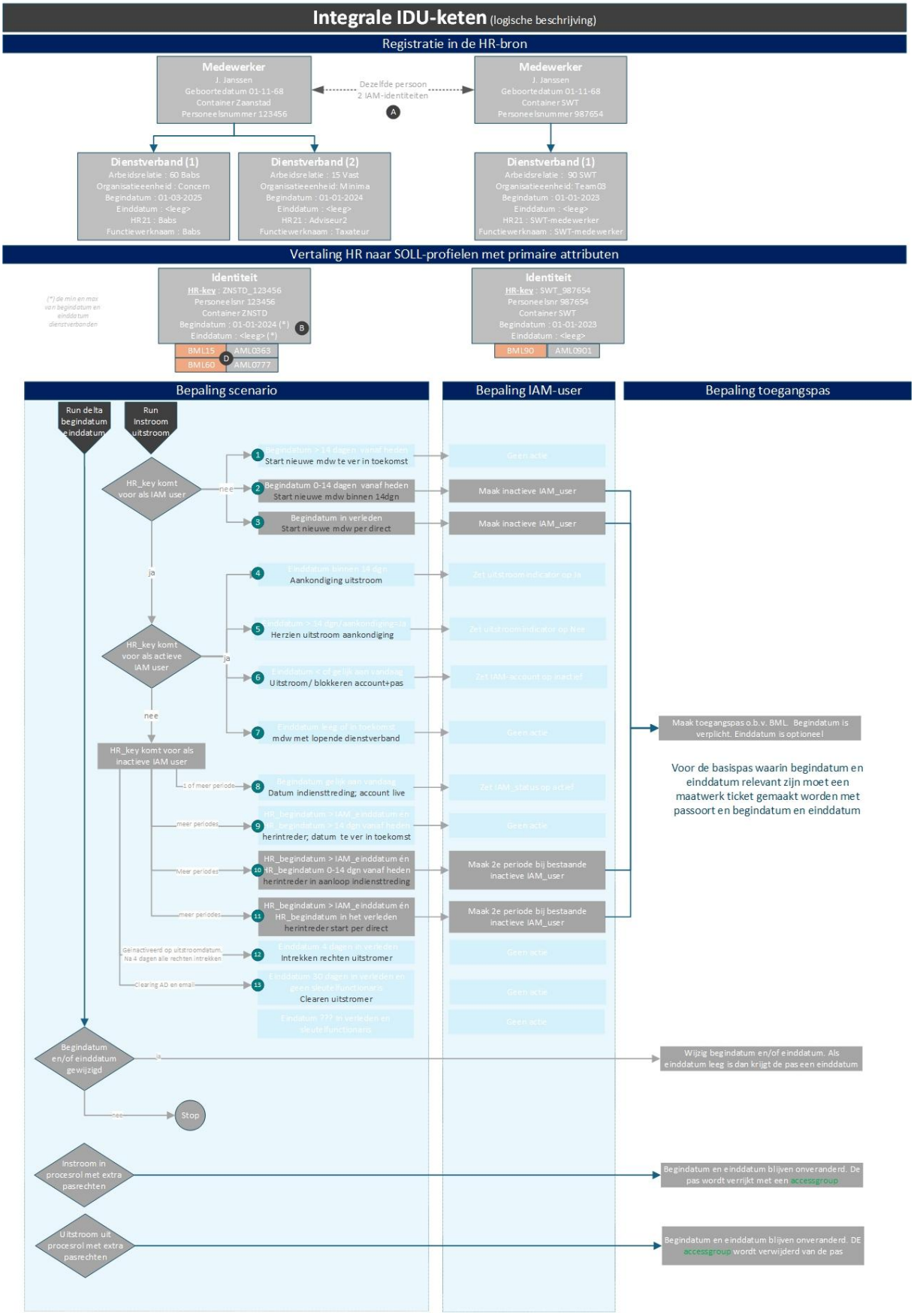
De nieuwe IAM-applicatie moet gekoppeld kunnen worden aan YouForce. Momenteel koppelt Gemeente Zaanstad o.b.v. een set xml-bestanden welke in bijlage 4 zijn beschreven. In de bijlage is ook gespecificeerd welke delen van de HR-administratie relevant zijn voor het IDU-proces.

2.3 Integrale IDU-keten

In onderstaande 3 schema's is in detail beschreven hoe onze IDU-keten nu functioneert. Wij willen deze werkwijze met het nieuwe systeem continueren. De beschreven keten moet werken voor instroom/uitstroom uit het HR-systeem maar ook voor instroom/uitstroom die ontstaat via directe invoer in een IAM-persoonskaart. Het is dus niet wenselijk dat – afhankelijk van het bronsysteem – er verschillende inrichtingen gemaakt/geprogrammeerd moeten worden in de IAM-applicatie. Voor meer details bijlage 3.

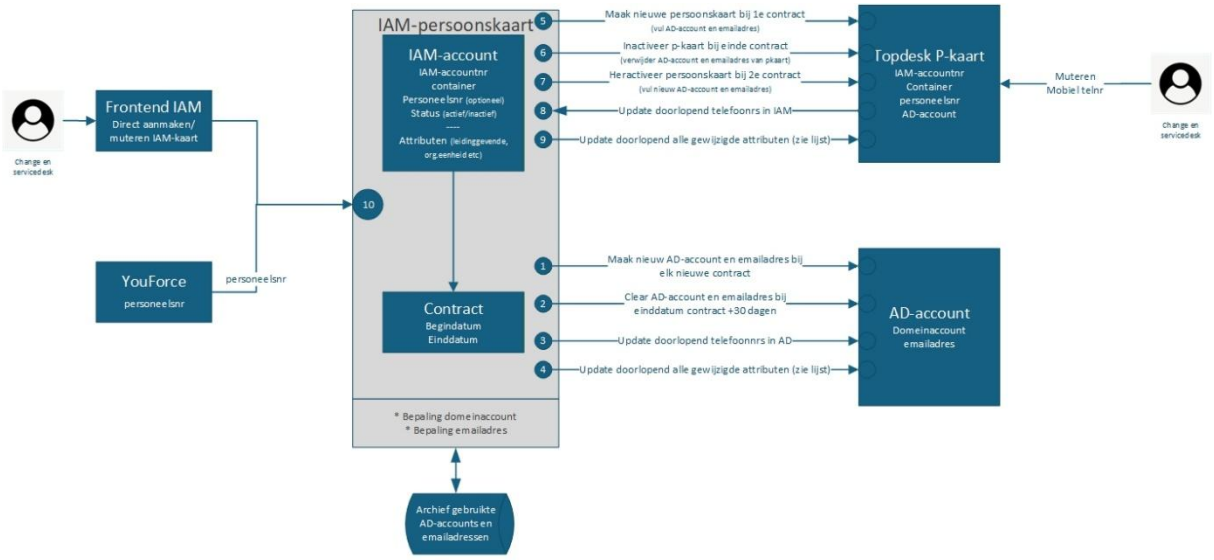


Figuur 3 Instroom, doorstroom en uitstroom (IDU-keten) van HR-bron t/m communicatie naar leidinggevende en medewerker



Figuur 4 -IDU keten specifiek voor toegangspassen

Toegangspassen en overige fysieke middelen worden via een ticket-based proces verwerkt (zie figuur 4). Toekenning, wijziging, blokkering en intrekking verlopen via een door de Oplossing gegenereerde opdracht of een ticket aan de verantwoordelijke uitvoering. Een directe technische koppeling tussen de Oplossing en een toegangspas- of pasjessysteem maakt geen onderdeel uit van de scope.



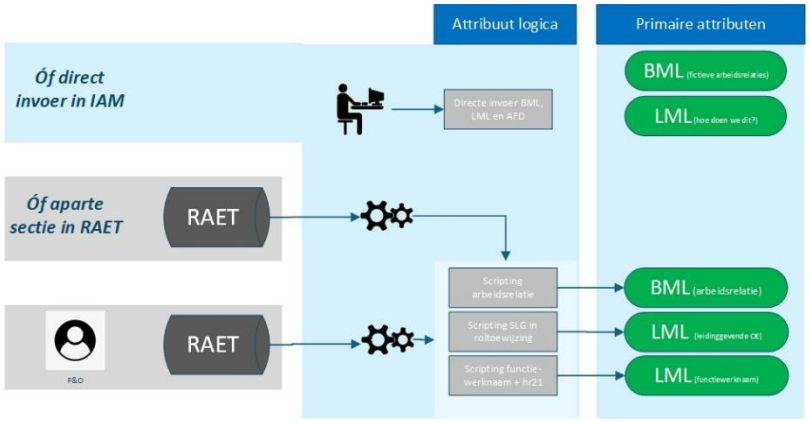
Nieuwe instroom
* IAM-persoonskaarten ontstaan vanuit Raet (koppeling) of handmatige invoer via de frontend van IAM **(10)**
    * Raet: indien personeelsnummer (HR-key) nog niet voorkomt in IAM dan wordt een IAM-persoonskaart aangemaakt
    * Via de front-end zal de beheerder o.b.v. naam, voorletter etc. moeten checken of er een nieuwe IAM-persoonskaart aangemaakt moet worden
* IAM bepaalt het eerstvolgende vrije 6-cijfige zaanstaddomeinaccount en eerstvolgende vrije emailadres.
* IAM maakt in AD een nieuw 6-cijferig AD-account en emailadres aan. IAM heeft een archieftabel waarin eerder gebruikte AD-accounts en emailadressen opgeslagen zijn. Deze mogen niet opnieuw gebruikt worden **(1)**
* In Topdesk wordt een nieuwe persoonskaart aangemaakt met daarin het IAM-accountnr en het Zaanstad domeinaccount en het emailadres **(5)**
* In Topdesk wordt het telefoonnummer ingevoerd. Gewijzigde telefoonnummers worden gedetecteerd en doorgezet naar IAM. IAM zet telefoonnummers door naar AD **(8,3)**
* Aanvullende attributen (leidinggevende, organisatie-eenheid, functie etc) komen in IAM binnen vanuit YouForce en worden doorlopend geupdated in Topdesk en AD **(4,9)**

Uitstroom
* IAM-account wordt geïnactiveerd op contract_einddatum. IAM-persoonskaart blijft met status inacief bestaan t.b.v. eventuele toekomstige herinstoom
* De AD-account wordt geïnactiveerd op contract_einddatum
* 30 dagen na contract_einddatum wordt AD-account gecleared (dus daadwerkelijk verwijderen AD-account plus data in email, onedrive, fileshares etc). **(2)**
* Het verwijderde AD-account en emailadres worden in een archieftabel opgeslagen zodat hergebruik niet meer kan voorkomen
* De Topdesk persoonskaart wordt geïnactiveerd 30 dagen na contract_einddatum. AD-account en emailadres worden verwijderd uit inactieve persoonskaart. **(6)**

Herinstroom (na 30 dagen)
* IAM-account wordt weer geactiveerd. Er wordt een tweede contractperiode toegevoegd.
* Er wordt een nieuw AD-account en een nieuw emailadres aangemaakt. Dit zal anders zijn dan het eerdere AD-account en emailadres die de her-instromer had. **(1)**
* De Topdesk persoonskaart wordt opnieuw geactiveerd. **(7)**
* Het nieuwe AD-account en emailadres worden ingevoegd in de geheractiveerde Topdesk persoonskaart **(7)**

Figuur 5 – IAM in relatie tot AD-accounts en TOPdesk-persoonskaarten

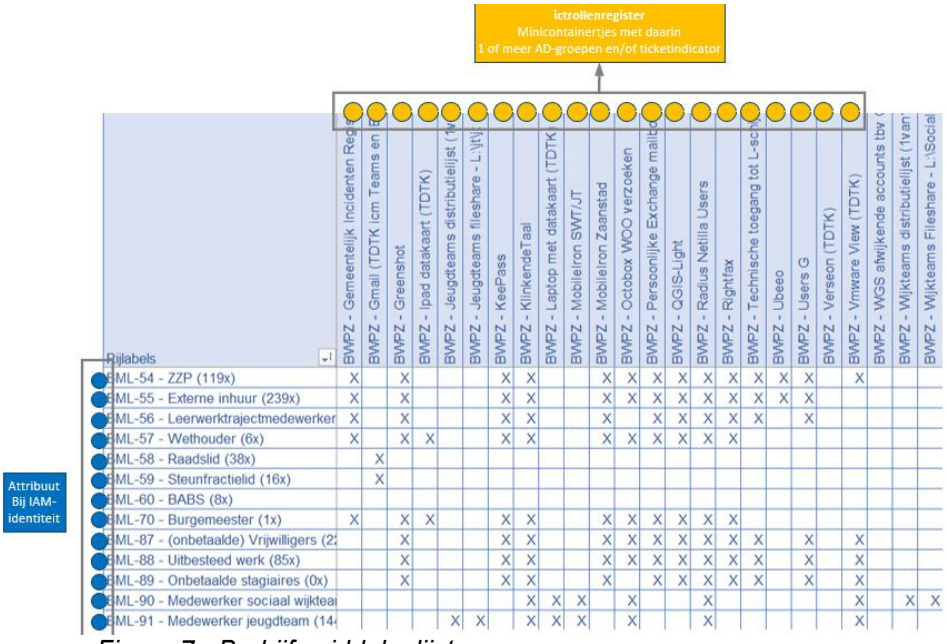
2.4 Bepalen HR-attributen



Figuur 6 Bepalen attributen o.b.v. HR-data

Zaanstad heeft een zgn. bedrijfsmiddelenlijst (BML) en een leidinggevenden middelenlijst (LML). Wij beschouwen BML (1 of meer waarden per IAM-account) en LML (ja/nee waarde) als attributen bij een IAM-account. De attributen moeten automatisch berekend worden bij ontvangst van gegevens uit het HR-systeem óf de attributen moeten door een beheerder direct ingevoerd kunnen worden op de IAM-persoonskaart.

Elke regel op een middelenlijst beschrijft een set autorisaties (applicaties met ICT-rollen) die verstrekt moet worden als een medewerker het betreffende attribuut heeft. In het geval van de bedrijfsmiddelenlijst kunnen medewerkers meerdere attributen binnen één lijst hebben. Dus vast in dienst (BML15) en Babs (BML60). Door wijzigingen in de HR-applicatie kunnen attributen wijzigen terwijl het IAM-account actief blijft.



Figuur 7 - Bedrijfsmiddelenlijst

2.5 Overrulen HR-koppeling

Er komen scenario's voor waarin vanuit IAM-perspectief de HR-koppeling overruled moet worden. Voorbeeld:

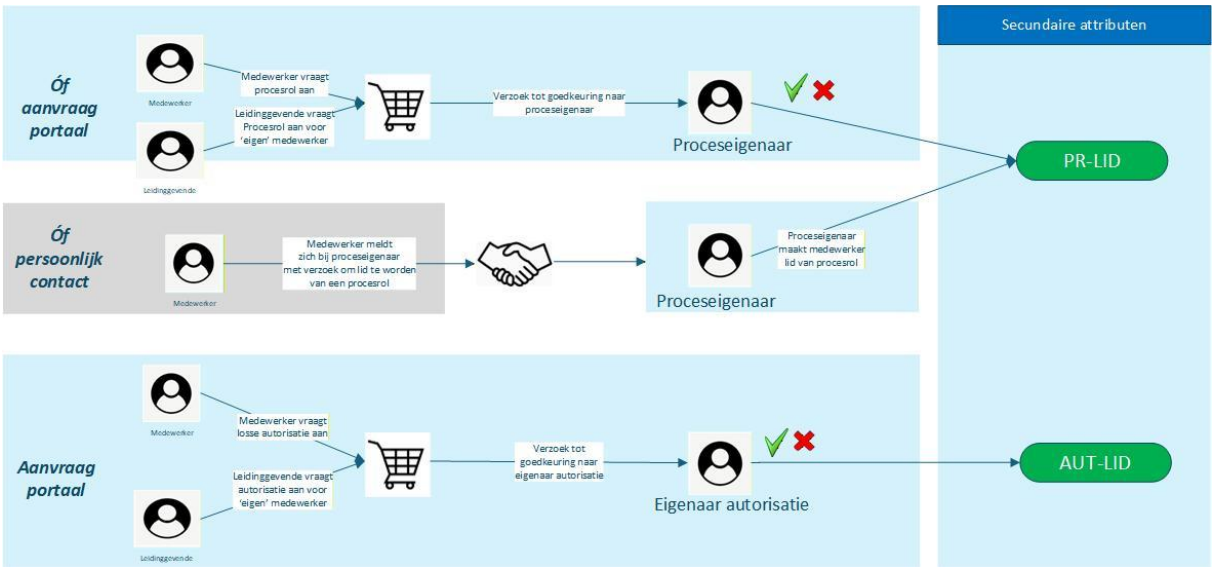
> Iemand wordt op staande voet ontslagen. Een geautoriseerde beheerder moet het account handmatig en onmiddellijk kunnen blokkeren. Daarbij worden het AD-account en de toegangspas direct inactief gezet. De reeds toegekende autorisaties worden op dat moment niet ingetrokken. Afhankelijk van de uitkomst van het ontslagonderzoek wordt de blokkering opgeheven of volgt de definitieve uitstroom via het HR-systeem. Bij definitieve uitstroom worden de autorisaties volgens het reguliere uitstroomproces ingetrokken.

2.6 Signalering doorstroom

Het verstrekken van rechten in applicatie vindt voor een groot deel plaats o.b.v. procesrollen. Medewerkers worden handmatig lid gemaakt van procesrollen. Het afmelden van procesrollidmaatschappen nadat iemand 'iets anders is gaan doen' binnen de organisatie wordt nogal eens vergeten. Hierdoor vervuilt de administratie en dat is ongewenst. Op dit moment gebeurt controle van de procesrollen door leidinggevenden halfjaarlijks handmatig (attestatie).

De gewenste signalering en ondersteuning van de periodieke controle van procesrollidmaatschappen is beschreven in wens W1B van het Programma van Eisen en Wensen. Wens W1B is voor deze functionaliteit leidend. De aangeboden functionaliteit moet bij inschrijving beschikbaar en demonstreerbaar zijn en, indien deze onderdeel is van de aangeboden Oplossing, uiterlijk op de overeengekomen implementatiedatum beschikbaar zijn.

3 Aanvragen en goedkeuren losse autorisaties en procesrollen



Figuur 7b Aanvragen procesrol op een intuïtieve en gebruiksvriendelijke wijze.

Het verstrekken van middelen vindt plaats op de volgende manieren:

- Verstrekken autorisaties op basis van attributen
    - De attributen worden óf berekend vanuit HR-data óf de attributen worden direct ingevoerd in de IAM-persoonskaart. De attributen zijn gekoppeld aan de bedrijfsmiddelenlijst of leidinggevendenlijst en alle autorisaties op deze middelenlijst worden automatisch verstrekt
- Aanvragen losse autorisatie

    Er zijn autorisaties die niet eenduidig verstrekt kunnen worden o.b.v. een attribuut of procesrol. Deze autorisaties moeten voor iedereen los aanvraagbaar zijn op een intuïtieve en gebruiksvriendelijke wijze. Een aantal van de aanvragen moet een goedkeuringsproces doorlopen.

- Aanvragen procesrollidmaatschappen.
    - Een procesrol geeft recht op een collectie autorisaties. In hoofdstuk 4 wordt beschreven hoe deze collecties samengesteld worden. Het lidmaatschap van een procesrol is niet af te leiden uit HR-data. Daarom moeten procesrollen op een intuïtieve en gebruiksvriendelijke wijze aanvraagbaar zijn door medewerkers, leidinggevenden en proceseigenaren. De proceseigenaar moet de aanvraag voor een procesrollidmaatschap altijd goedkeuren voor de autorisaties daadwerkelijk verleend worden.

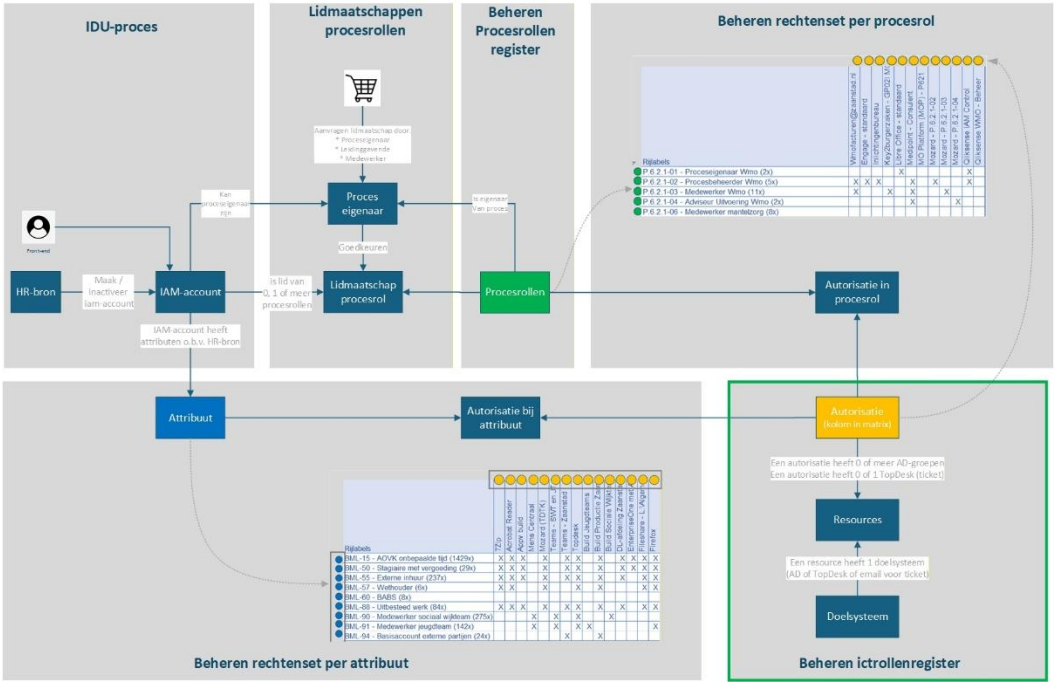
4 IAM-beheer

Gemeente Zaanstad wil 2 registers beheren in de nieuwe IAM-applicatie
- ICT-rollenregister
- Procesrollenregister

Door beide registers te combineren ontstaan matrices. Er zijn 2 soorten matrices:
- Procesrolmatrices
- Attribuutmatrices

4.1 Beheren ICT-rollenregister

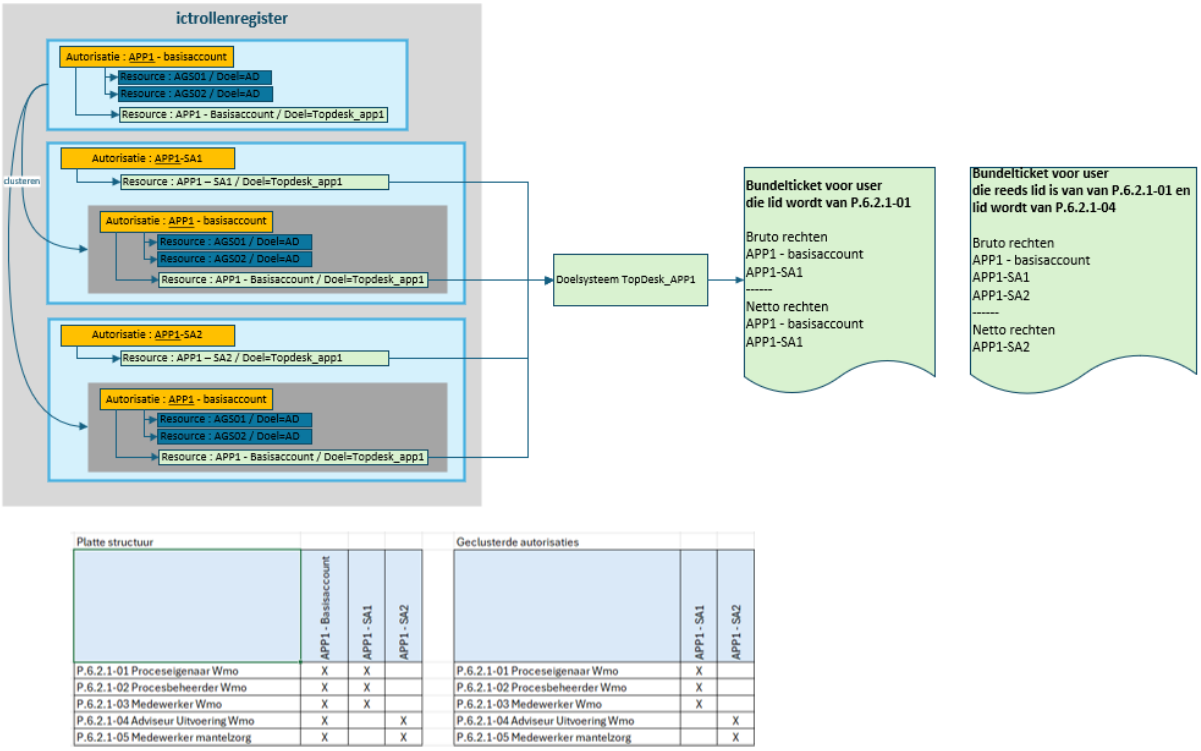
In het ICT-rollenregister worden alle applicaties inclusief de autorisatiestructuur *in* de applicatie geadministreerd. Het ICT-rollenregister heeft verbindingen met:
- Beheren rechtenset per procesrol
- Beheren rechtenset per attribuut



Figuur 8 Scope beheren ICT-rollenregister

4.2 Functionaliteit ICT-rollenregister

Het ICT-rollenregister bestaat uit:
- Autorisaties (lichtblauwe kaders)
- Resources (donkerblauwe en lichtgroen binnen licht blauwe kaders)
- Doelsystemen (donkerblauw is AD en lichtgroen is TOPdesk)



Platte structuur

	APP1 - Basisaccount	APP1 - SA1	APP1 - SA2
P.6.2.1-01 Proceseigenaar Wmo	X	X	
P.6.2.1-02 Procesbeheerder Wmo	X	X	
P.6.2.1-03 Medewerker Wmo	X	X	
P.6.2.1-04 Adviseur Uitvoering Wmo	X		X
P.6.2.1-05 Medewerker mantelzorg	X		X

Geclusterde autorisaties

	APP1 - SA1	APP1 - SA2
P.6.2.1-01 Proceseigenaar Wmo	X	
P.6.2.1-02 Procesbeheerder Wmo	X	
P.6.2.1-03 Medewerker Wmo	X	
P.6.2.1-04 Adviseur Uitvoering Wmo		X
P.6.2.1-05 Medewerker mantelzorg		X

Figuur 9 Schematische weergave ICT-rollenregister inclusief het concept 'gebundelde tickets'

4.3 Definities ICT-rollenregister

Level 1-rechten	Om te kunnen werken in een applicatie is vrijwel altijd een basisaccount nodig. Vaak wordt dit basisaccount verstrekt via een AD-groep maar het kan ook handmatig verstrekt worden door een beheerder o.b.v. een TOPdesk-ticket. Ook kan een combinatie voorkomen: de user wordt in een AD-groep geplaatst, maar de functioneel beheerder moet ook een ticket ontvangen om handmatig nog enkele rechten in te regelen. In dit document wordt het basisaccount level 1-rechten genoemd.
Level 2-rechten	Naast een basisaccount krijgt een user vrijwel altijd een specifieke ICT-rol. Dus resources ín de applicatie. In dit document wordt dit level 2 genoemd. In de procesmatrices wordt alleen level 2 genoemd. Dit is herkenbaar voor functioneel beheer en het is evident dat er voorafgaand aan level 2-rechten ook altijd een basisaccount (level 1) verstrekt moet worden.
Geneste autorisaties (level 1 in level 2)	Vakapplicaties hebben naast een basisaccount vaak meerdere functionele autorisaties. De basisautorisatie moet slechts éénmaal worden ingericht en beheerd en automatisch worden meegeleverd bij de relevante functionele autorisaties en procesrollen van dezelfde applicatie. Dit kan worden gerealiseerd door nesting, overerving of een andere functioneel gelijkwaardige standaardinrichting. Technische nesting is geen doel op zich. Het beoogde resultaat is dat het basisaccount niet afzonderlijk in iedere procesrol hoeft te worden opgenomen en dat wijzigingen in de basisautorisatie op één plaats kunnen worden beheerd.

4.4 Definities vertaald naar voorbeeld

De definities zoals hiervoor beschreven zijn in dit hoofdstuk vertaald naar een voorbeeld.

Autorisaties	Geneste autorisatie (basisaccount)
Key2begraven - basisaccount	
Key2begraven - Beheer (niet gespecificeerd)	Key2begraven - basisaccount
Key2begraven - Muteren	Key2begraven - basisaccount
Key2begraven - Raadplegen	Key2begraven - basisaccount
Key2begraven - Webagenda	Key2begraven - basisaccount

Hierboven 5 autorisaties behorende bij de applicatie *key2begraven*. Vier autorisaties zijn level 2 (rechten ín de applicatie) en één autorisatie is level 1, n.l. het basisaccount van de applicatie.

In dit voorbeeld is het basisaccount *Key2begraven – basisaccount* gekoppeld aan vier functionele autorisaties. De getoonde nesting is één mogelijke technische realisatie. Een andere inrichting is toegestaan wanneer het basisaccount slechts éénmaal hoeft te worden beheerd en automatisch wordt meegeleverd bij de relevante functionele autorisaties en procesrollen.

Doelsysteem	Userbeheergroep	ID_wijzigingssjabloon (fictieve nrs)
Topdesk (Key2begraven)	FB Belastingen	102
Topdesk (Key2betalen)	FB Frontoffice	107
Topdesk (Key2burgerzaken)	FB Frontoffice	107
Topdesk (Key2GBA-V)	FB Frontoffice	107

De applicatie *TOPdesk (key2begraven)* staat in de lijst doelsystemen. Rechten in *key2begraven* worden gecommuniceerd via TOPdesk aan een functioneel beheerder. De tickets worden als *wijzigingssjaboon* doorgezet naar TOPdesk. Elk doelsysteem heeft een ID wat correspondeert met de ID van de behandelgroep in TOPdesk.

Elke applicatie waarbij de rechten handmatig worden verstrekt heeft een eigen doelsysteem met de syntax *[TOPdesk][naam_applicatie]*. Dit is de basis voor het intelligente script voor het genereren van ticketteksten en het maken van bundeltickets. Zou het doelsysteem alleen *TOPdesk* heten (wat technisch gezien feitelijk het geval is) dan zijn de resources niet per applicatie te onderscheiden en dat is ongewenst.

Autorisaties	Resource (nu nog meer AD-groepen in 1 veld, moet per regel worden)	Doelsysteem
Key2begraven - basisaccount	SSO Begraven, AGS-Key2Begraven-10.1-NL-U, AGS-MDU-5-NL-U	AD
Key2begraven - basisaccount	Key2begraven - basisaccount	Topdesk (Key2begraven)
Key2begraven - Beheer (niet gespecificeerd)	Key2begraven - Beheer (niet gespecificeerd)	Topdesk (Key2begraven)
Key2begraven - Muteren	Key2begraven - Muteren	Topdesk (Key2begraven)
Key2begraven - Raadplegen	Key2begraven - Raadplegen	Topdesk (Key2begraven)
Key2begraven - Webagenda	Key2begraven - Webagenda	Topdesk (Key2begraven)

Aan de autorisaties zijn resources gekoppeld. De autorisatie *Key2begraven – basisaccount* heeft 2 AD-groepen in het doelsysteem *AD* en 1 resource in doelsysteem *TOPdesk (key2begraven)*.

Procesrolnr	Autorisatie	Procesrolnaam (aantal users)
O.3.2.1.C-05	Key2begraven - Beheer (niet gespecificeerd)	O.3.2.1.C-05 - Beheerder Belastingen (7x)
P.1.1.2-05	Key2begraven - Raadplegen	P.1.1.2-05 - Specialist groen/waterhuishouding (2x)
P.7.1.1-01	Key2begraven - Raadplegen	P.7.1.1-01 - Proceseigenaar Heffen en Invorderen (1x)
P.7.1.1-02	Key2begraven - Raadplegen	P.7.1.1-02 - Procesbeheerder Heffen en Invorderen (1x)
P.7.1.1-07	Key2begraven - Muteren	P.7.1.1-07 - Specialist/Expert Heffen (19x)
P.8.3.3-01	Key2begraven - Raadplegen	P.8.3.3-01 - Proceseigenaar Exploiteren begraafplaatsen en urnentuin (1x)
P.8.3.3-02	Key2begraven - Raadplegen	P.8.3.3-02 - Procesbeheerder Exploiteren begraafplaatsen en urnentuin (5x)
P.8.3.3-03	Key2begraven - Muteren	P.8.3.3-03 - Medewerker grafrechten (3x)
P.8.3.3-03	Key2begraven - Webagenda	P.8.3.3-03 - Medewerker grafrechten (3x)
P.8.3.3-04	Key2begraven - Raadplegen	P.8.3.3-04 - Medewerker begraafplaatsen (6x)
P.8.3.3-05	Key2begraven - Raadplegen	P.8.3.3-05 - Beheerder begraafplaatsen (3x)
P.8.3.3-06	Key2begraven - Raadplegen	P.8.3.3-06 - Adviseur beleid begraafplaatsen (0x)

Autorisaties worden gekoppeld aan procesrollen en attributen. Opmerkingen:

- Alleen level 2-autorisaties zijn gekoppeld aan de procesrollen. Het basisaccount (level 1) wordt automatisch meegenomen wanneer een relevante level 2-autorisatie via een procesrol

wordt toegekend. Dit mag door nesting of door een functioneel gelijkwaardige inrichting worden gerealiseerd.

- Procesrollen kunnen meerdere autorisaties hebben in één applicatie (zie b.v. P.8.3.3-03). De rechten moeten in één ticket gecommuniceerd worden naar TOPdesk

Procesrolnr	Gebruikerscode	Procesrolnr	Gebruikerscode
O.3.2.1.C-05	USER0387	P.7.1.1-07	USER1556
O.3.2.1.C-05	USER0388	P.7.1.1-07	USER1557
O.3.2.1.C-05	USER0389	P.7.1.1-07	USER1558
O.3.2.1.C-05	USER0390	P.7.1.1-07	USER1559
O.3.2.1.C-05	USER0210	P.7.1.1-07	USER1560
O.3.2.1.C-05	USER0317	P.7.1.1-07	USER1561
O.3.2.1.C-05	USER0391	P.8.3.3-01	USER1203
P.1.1.2-05	USER0654	P.8.3.3-02	USER1548
P.1.1.2-05	USER0655	P.8.3.3-02	USER1549
P.7.1.1-01	USER1543	P.8.3.3-02	USER1552
P.7.1.1-02	USER0560	P.8.3.3-02	USER1553
P.7.1.1-07	USER1544	P.8.3.3-02	USER1556
P.7.1.1-07	USER1545	P.8.3.3-03	USER0193
P.7.1.1-07	USER1546	P.8.3.3-03	USER0195
P.7.1.1-07	USER1547	P.8.3.3-03	USER0209
P.7.1.1-07	USER1548	P.8.3.3-04	USER1229
P.7.1.1-07	USER1549	P.8.3.3-04	USER1234
P.7.1.1-07	USER0560	P.8.3.3-04	USER0197
P.7.1.1-07	USER1550	P.8.3.3-04	USER1628
P.7.1.1-07	USER1551	P.8.3.3-04	USER1249
P.7.1.1-07	USER1552	P.8.3.3-04	USER1254
P.7.1.1-07	USER1553	P.8.3.3-05	USER1260
P.7.1.1-07	USER1554	P.8.3.3-05	USER1216
P.7.1.1-07	USER1555	P.8.3.3-05	USER1153

Users worden gekoppeld aan één of meer procesrollen.

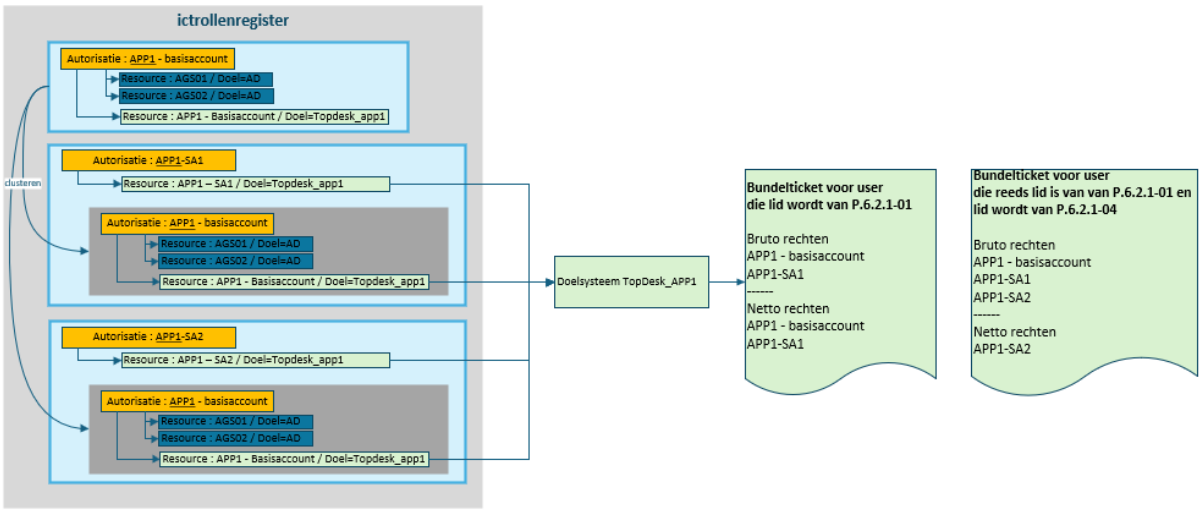
4.5 Gelaagde autorisatiestructuur – uitwerking voorbeeld

Gemeente Zaanstad verstrekt via IAM niet alleen de toegang tot de applicatie (basisaccount) maar verstrekt ook opdrachten via TOPdesk om ICT-rollen *ín* de applicatie toe te kennen.

De opdracht voor een basisaccount kan eenvoudig verstrekt worden vanuit een IAM-applicatie, maar het – in samenhang – verstrekken van een basisaccount plus de resources (ICT-rollen) *ín* de applicaties is minder vanzelfsprekend. Daarbij moet ook nog rekening gehouden worden met het volgende: een medewerker wordt lid van procesrol-A en krijgt een basisaccount plus rechten in de applicatie. In een later stadium wordt de medewerker lid van een procesrol-B waarin aanvullende rechten in de applicatie gegeven moeten worden.

In de opdracht die voortkomt uit procesrol-B moeten zowel de gevraagde wijziging, de delta, als de reeds toegekende rechten binnen de betreffende applicatie inzichtelijk zijn. De delta moet duidelijk worden onderscheiden van de reeds bestaande rechten. Een andere presentatievorm is toegestaan, mits zowel de bestaande situatie als de uit te voeren wijziging ondubbelzinnig uit het Bundelticket blijken.

Wanneer voor één applicatie meerdere resources moeten worden toegekend of ingetrokken, worden deze gezamenlijk in één Bundelticket verwerkt. Het is niet de bedoeling dat per afzonderlijke resource een apart ticket wordt aangemaakt.



Platte structuur

	APP1 - Basisaccount	APP1 - SA1	APP1 - SA2
P.6.2.1-01 Proceseigenaar Wmo	X	X	
P.6.2.1-02 Procesbeheerder Wmo	X	X	
P.6.2.1-03 Medewerker Wmo	X	X	
P.6.2.1-04 Adviseur Uitvoering Wmo	X		X
P.6.2.1-05 Medewerker mantelzorg	X		X

Geclusterde autorisaties

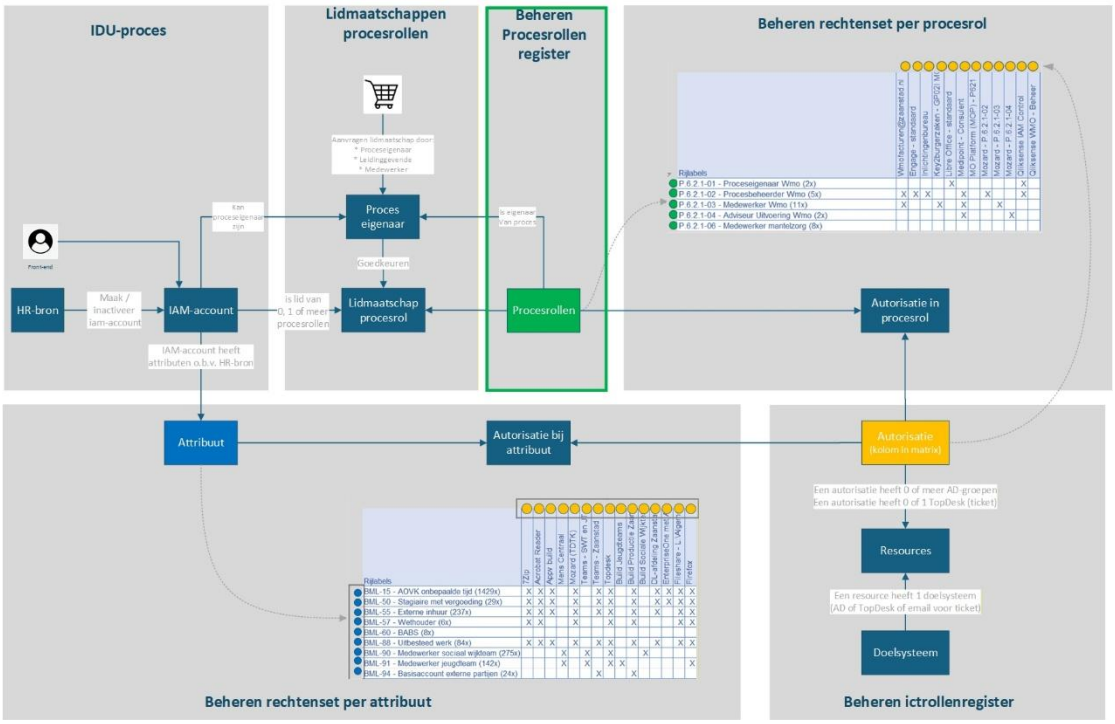
	APP1 - SA1	APP1 - SA2
P.6.2.1-01 Proceseigenaar Wmo	X	
P.6.2.1-02 Procesbeheerder Wmo	X	
P.6.2.1-03 Medewerker Wmo	X	
P.6.2.1-04 Adviseur Uitvoering Wmo		X
P.6.2.1-05 Medewerker mantelzorg		X

Figuur 11 Bundeltickets

In bovenstaande schema is het vraagstuk van de gelaagde datastructuur weergegeven. Voor de applicatie APP1 zijn er 3 autorisaties:

- APP1 – basisaccount
- APP-SA1 (ict-rol / gebruikersprofiel 1 in APP1)
- APP-SA2 (ict-rol / gebruikersprofiel 2 in APP1)

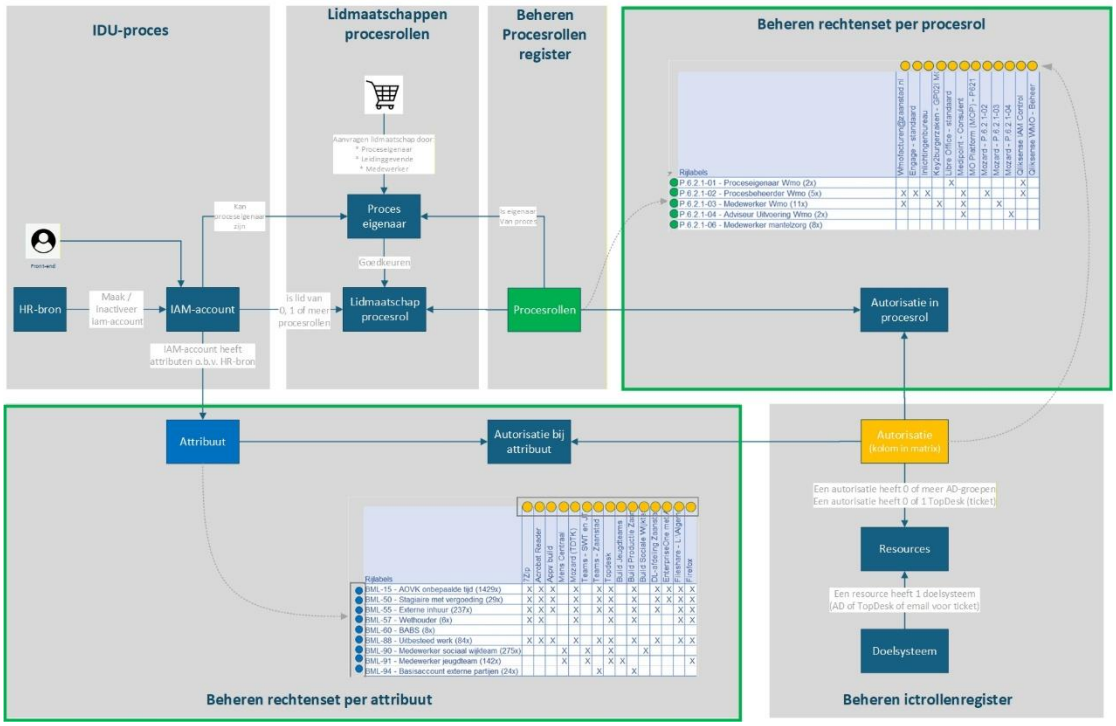
4.6 Beheren procesrollen



Figuur 10 Beheren procesrollen

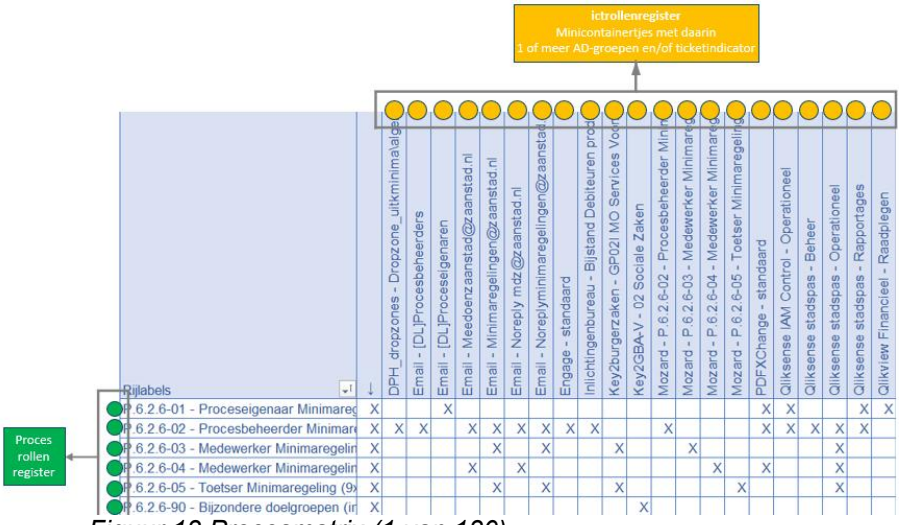
Zaanstad heeft een processenhuis met 130 processen. Binnen een proces bestaan gemiddeld 5-7 procesrollen. Per jaar komen er ongeveer 10-15 procesrollen bij. Deze wijzigingen worden doorgevoerd in het procesrollenregister en moeten ook in de IAM-applicatie worden verwerkt.

4.7 Beheren procesrolmatrices en attribuutmatrices

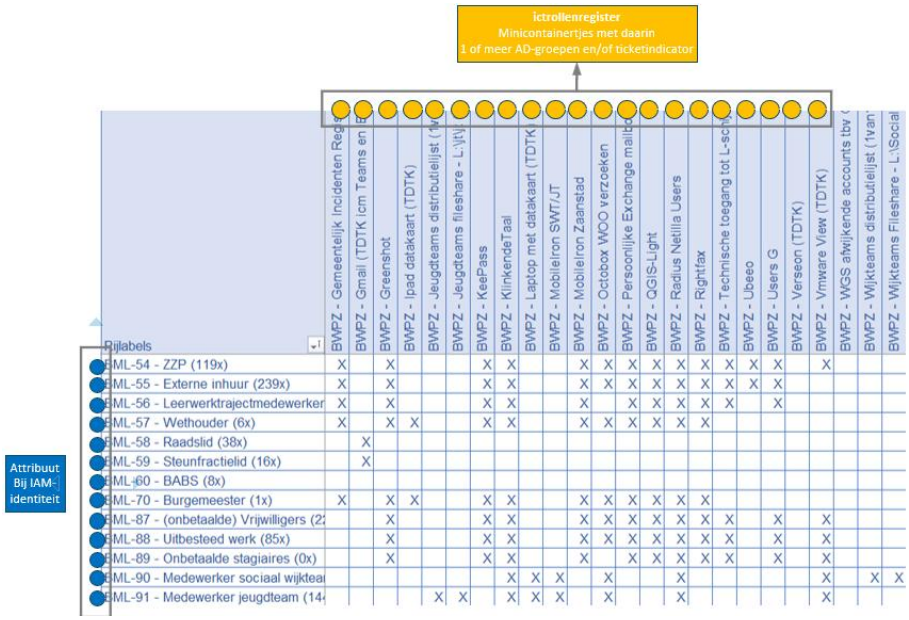


Figuur 12 beheren proces- en attribuutmatrices

Hieronder worden 2 matrices getoond: een procesrolmatrix en een attribuutmatrix. De (geeloranje) kolommen zijn autorisaties uit het ICT-rollenregister. In figuur 13 zijn de regels de procesrollen uit het procesrollenregister (groen) en in figuur 14 zijn de regels attributen uit de IAM-persoonskaart (blauw).



Figuur 13 Procesmatrix (1 van 130)



Figuur 14 Bedrijfsmiddelenmatrix

5 Conversie

De bestaande autorisatiestructuur uit Gov4Gem vormt het uitgangspunt voor de initiële inrichting en migratie. De implementatie betreft het overnemen en inrichten van deze bestaande structuur in de nieuwe Oplossing. Een fundamentele aanpassing of herinrichting van de bestaande autorisatiestructuur, procesrollenstructuur of governance maakt geen onderdeel uit van de implementatie. De beschikbaar gestelde voorbeeld-conversiedata in Bijlage 15 (buiten dit document) geven inzicht in de opbouw van de huidige autorisatiestructuur en de migratie-uitgangspunten.

- **Autorisatieregister**

Autorisaties en resources	
Autorisatienaam	
Resourcenaam	
Doelsysteem_id	

Doelsysteem	
Doelsysteem_id	
Doelsysteemnaam	Ad, TOPdesk (ssd), TOPdesk (mozard) etc
Provisioning_methode	AD, ticket of email

- **Procesrollen**

Procesrollen	
Procesrolnummer	
Procesrolnaam	

- **Autorisatie in procesrollen**

Autorisatie in procesrol	
Autorisatie	
Procesrolnummer	P.6.2.4-02

- **Autorisatie in attributen**

Autorisatie in attribuut	
Autorisatie	
Attribuut	BML15, LML01

- **User in procesrol**

User in procesrol	
User_id	
Container	
Naam	
Voorletters	
Organisatieonderdeel_level1_id	Linkt aan basistabel
Organisatieonderdeel_level2_id	Linkt aan basistabel; level 2 kan leeg zijn
Organisatieonderdeel_level3_id	Linkt aan basistabel; level 3 kan leeg zijn
iam_begindatum	
iam_einddatum	Kan leeg zijn

- **User met attribuut**

User kan meerdere attributen hebben dus ook meerdere records in dit bestand.

User met attribuut	
User_id	
Attribuut	BML15, LML01 etc
Attribuut_begindatum	
Attribuut_einddatum	Kan leeg zijn

- **User in procesrol**

User in procesrol	
User_id	
Procesrolnummer	P.6.2.4-02

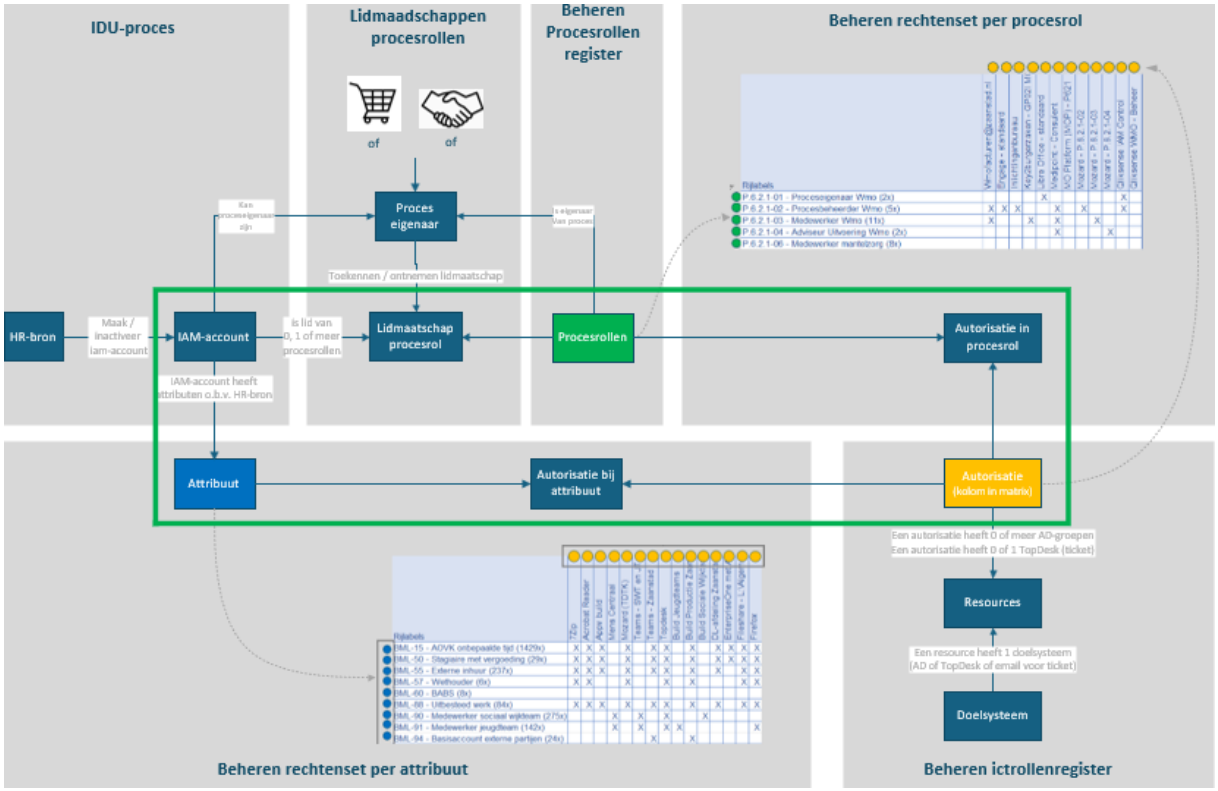
- **User met losse autorisatie**

Losse autorisaties zijn de uitzondering. Echter, deze komen wel voor als het verstrekken van autorisaties via procesrol of attribuut niet passend is.

User met losse autorisatie	
User_id	
Autorisatie	Visio
Autorisatie_begindatum	
Autorisatie_einddatum	Kan leeg zijn

Bijlagen

Bijlage 1 IAM-persoonskaarten



Scope van IAM-persoonskaart

Bijlage 2 Identiteitscontainers

De definitieve indeling van de identiteitscontainers wordt tijdens de implementatie in overleg met Opdrachtnemer vastgesteld. Als indicatieve inrichting wordt uitgegaan van één identiteitscontainer voor Gemeente Zaanstad, afzonderlijke containers voor Stichting Jeugdteam en Sociaal Wijkteam en één gezamenlijke container voor de overige partnerorganisaties. Deze indeling is een nadere concretisering binnen de bestaande scope. De Oplossing moet containers flexibel en beheersbaar kunnen inrichten en wijzigen.

Naar verwachting zullen minder dan 20 personen gelijktijdig in meerdere containers voorkomen en dat dit veelal een tijdelijke doorstroomsituatie betreft.

Bijlage 3 Koppeling AD

IAM en AD zijn geconnecteerd via domain zaanstad.gem.local op domain controller MDC01Z.

De attributen die in AD worden geregistreerd en uitgelezen door IAM zijn:

Veldnaam	Omschrijving	Bron
accountExpires	Waarde '(never)'	IAM
sn	Achternaam	IAM
given_name	Voornaam	IAM
initials	Voorletters	IAM
extensionAttribute2	Voorvoegsels	
cn	Samengestelde naam (achternaam, voornaam voorvoegsel)	IAM
displayname	Samengestelde naam (achternaam, voornaam voorvoegsel)	IAM
name	Samengestelde naam (achternaam, voornaam voorvoegsel)	IAM
distinguishedname	CN=[achternaam]\, [voornaam],OU=Zaanstad,OU=Users,OU=User Accounts,DC=zaanstad,DC=gem,DC=local	IAM
extensionAttribute3	Geslacht	IAM
objectGuid	UID	AD
mail	E-mail	IAM
extensionAttribute5	Waarde 'znstd_standaard' 'znstd_parkeerplaats' of 'znstd_sleutelfiguur'	IAM
company	Organisatieonderdeel	IAM
extensionAttribute6	Organisatieonderdeel	IAM
office	Afdeling	IAM
extensionAttribute7	Afdeling	IAM
extensionAttribute8	Team	IAM
department	Team	IAM
title	Functie (werknaam)	IAM
mailNickname	UserId	IAM
samAccountname	UserId	IAM
streetaddress	Locatie (Stadhuis)	IAM
proxyAdresses	Proxyadressen	IAM
manager	CN=[achternaam manager/,voornaam voorvoegsel manager] ,OU=Zaanstad,OU=Users,OU=User accounts,DC=zaanstad,DC =gem,DC=local	IAM
msExchHideFromAddressLists	False	AD
l	Plaats (Zaandam)	IAM
postalCode	Postcode 1506 MZ (alleen voor Zaanstad medewerkers)	IAM
homedrive	Waarde 'U:'	IAM
homedirectory	\\zaanstad.gem.local\data\user\[UserId]	IAM
profilePath	Profielpad (\\zaanstad.gem.local\fslogic$\profiles\[userid])	IAM
legacyExchangeDN	/o=Gemeente Zaanstad/ou=External (FYDIBOHF25SPDLT)/cn=Recipients/cn=9446e824f1a943cb89884b448a182bf3	IAM
pager	Printercode (5-cijferige unieke waarde)	IAM
extensionAttribute15	Printercode (5-cijferige unieke waarde)	IAM
homePhone	Telefoonnummer	IAM
telephoneNumber	Telefoonnummer	IAM
mobile	Mobiel nummer	IAM

Voor de verschillende identiteiten worden in AD de onderstaande OU's gehanteerd :

Identiteit	Naam OU
Zaanstad / Vast dienstverband, externe inhuur, ZZP, stagiaires, leerwerktraject, etc.	User accounts\Users\Zaanstad
Sociale Wijkteams en Jeugdteams	User accounts\Users\Sociale Wijkteams
Pact medewerkers	User accounts\Users\Pact Zaandam
Medewerkers Omgevingsdienst , Overgemeenten, Leveranciers I&S, Werkom	User accounts\Users\Basisaccount externe partijen

Accounts worden bij offboarding vier dagen na de datum van uitdiensttreding gedeactiveerd en verplaatst naar de OU ‘Medewerker uitdienst’. Dertig dagen na de datum van uitdiensttreding worden de accounts verwijderd.

Het organisatieonderdeel, afdeling en team worden op dezelfde manier geregistreerd als beschreven in de IAM – TOPdesk koppeling.

Bijlage 4 Koppeling YouForce

Voor de koppeling tussen YouForce en IAM wordt gebruik gemaakt van zgn. BINT (Beaufort INTerface) bestanden (technisch XML). In de toekomst zal hier mogelijk een API koppeling voor worden gebruikt.

Deze BINT-bestanden bevatten vier verschillende soorten bestanden, t.w.

- Roltoewijzing : deze bevat de gegevens van de leidinggevenden (1x)
- Organisatie–eenheden : alle organisatie-eenheden die in YouForce voorkomen (1x)
- Functie – alle hr21-functies (1x)
- Medewerkergegevens – alle resterende medewerkergegevens (125 x)

Deze BINT-bestanden worden momenteel twee maal per dag aangeleverd, met daarin de gegevens uit het HR systeem m.b.t. de volgende arbeidsrelaties :

01 – Toekomstig medewerker
10 – Vast publiekrechtelijk
15 - AOVK onbepaalde tijd
20 – Tijdelijk publiekrechtelijk
25 - AOVK bepaalde tijd
30 – BBL overeenkomst
50 – Stageovereenkomst
51 – Stage onbetaald
52 – Fractie-assistent
53 – Stagiaires onbetaald
54 – ZZP
55 – Externe inhuur
56 – Leerwerktraject betaald
57 – Wethouder
58 – Raadslid
59 – Steunfractielid
60 – BABS medewerker
70 – Burgemeester
80 – Niet opting-inn (vooral raadsleden/fractieleden)

De medewerkers met onderstaande arbeidsrelatie worden niet meegenomen in de BINT bestanden :
83 – Pensioen gem. zaanstad (waaronder voormalig bestuurders)
99 – Geen dienstverband (waaronder wachtgelders)

Onderstaande gegevens worden in de BINT bestanden vermeld, waarvan slechts de aangegeven velden in IAM worden gebruikt.

Nr	Rubriek in YouForce / Bint	Registratie In IAM
P00301	Geboortenaam	X
P00302	Geboortenaam - voorvoegsels	X
P00303	Voorletters	X
P00304	Gebruik achternaam	X
P00305	Titulatuur voor de naam	
P00321	Geboortedatum	X
P00322	Datum in dienst	X
P00329	Burgerlijke staat	X
P00330	Geslacht	X
P00390	Partner achternaam	X
P00391	Partner voorvoegsel	X
P00404	Percentage deelbetrekking	
P00830	Datum uit dienst	X
P01001	Persoonsnummer	X

P01002	Voornamen	
P01003	Roepnaam	X
P01004	Nationaliteit	
P01008	Samengestelde naam	X
P01009	Samengestelde naam-voorvoegsels	X
P01014	Woonadres - straatnaam	
P01016	Woonadres – Huisnummer	
P01018	Woonadres – Huisnummertoev.	
P01020	Woonadres – Postcode	
P01022	Woonadres – Plaatsnaam	
P01024	Woonadres – Landcode	
P01027	Woonadres - Telefoonnummer	
P01036	Telefoonnummer mobiel	
P01037	Telefoonnummer werk	
P01038	Faxnr prive	
P01039	Faxnr werk	
P01101	Volgnr dienstverband	
P01103	Opdrachtgever	X
P01106	Hierarchische org.eenheid	X
P01107	Primaire functie	X
P01109	Uren per week	
P01121	Operationele org. eenheid	X
P01122	Operationele functie	X
P01123	Soort inzet	
P01124	Uren inzet per week	
P01125	Ingang inzet	X
P01126	Einde inzet	X
P03937	Titulatuur achter de naam	
P00306	Tussenvoegsel (zie voorvoegsel)	
P01131	Regelnr Loonverdeling	
P01134	Kostenplaats Iv	
P01133	Kostensoort	
P01050	Locatie	
P01102	Soort arbeidsrelatie	X
ER3001	Functie (werknaam)	X

Daarnaast registreert IAM nog een tweetal velden welke worden gebruikt als extra criteria voor het verstrekken van bepaalde rechten uit de BML.

Naam veld	**Omschrijving**
Type medewerker	Zaanstad, Uitbesteed werk, Sociaal Wijkteam, Jeugdteam, Onbetaalde stagiair, vrijwilliger, PACT medewerker of Externe Partij *
Meta eigenaar (bron van gegevens)	Handmatig of uit YOUFORCE/HR (FORM / system_HR)

* Voor medewerkers uit YOUFORCE wordt het type ‘Zaanstad’ gebruikt, en system_HR voor ‘Meta eigenaar’

Voor (in IAM) handmatig ingevoerde medewerker-gegevens worden de volgende (fictieve) arbeidsrelaties gehanteerd (welke niet in YOUFORCE voorkomen :

87 - Vrijwilliger
88 – Uitbestede medewerker
89 – Leerwerktraject onbetaald
90 – Sociale Wijkteams
91 – Jeugdteams

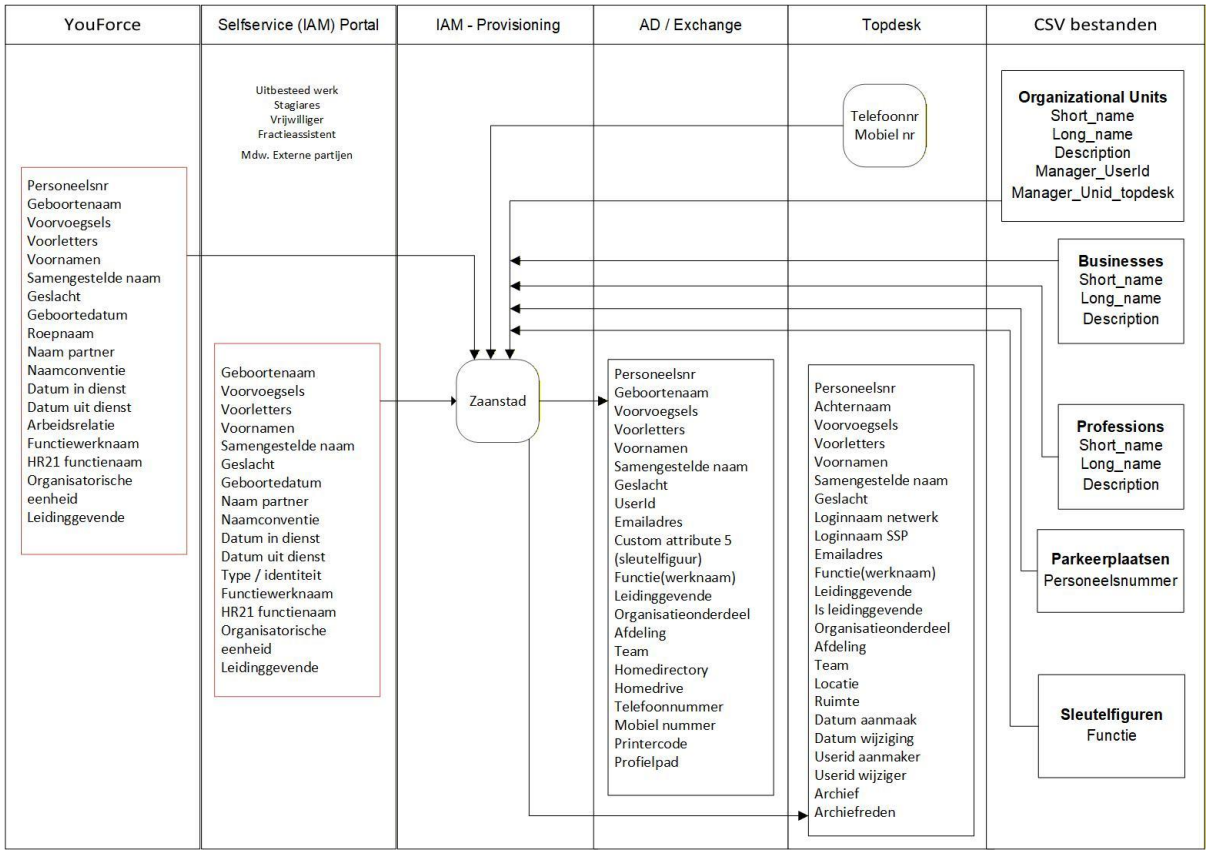
93 – PACT medewerkers
94 – Externe partijen

Bijlage 5 Koppeling TOPdesk

Inleiding

De koppeling tussen IAM en TOPdesk betreft een API-koppeling waarbij in beide richtingen gegevens worden uitgewissel:

- Vanuit IAM-provisioning naar TOPdesk worden gegevens gepushed:
  - YouForce (kolom 1), IAM (kolom 3) naar TOPdesk (kolom 5)
  - Selfservice portaal (kolom 2), IAM (kolom 3) naar TOPdesk (kolom 5)
- Vanuit TOPdesk via IAM-provisioning naar AD worden gegevens gepushed:
  - TOPdesk (kolom 5), IAM (kolom 3) naar AD (kolom 4) bij On-Premise ~~of Microsoft Entra ID bij SaaS~~.



Koppeling IAM -> TOPdesk
Onderstaande velden moeten door de iam koppeling in TOPdesk worden gevuld en gewijzigd bij het instroom- en doorstroom-proces:

De unieke sleutel voor een persoonskaart is IAM_account. Indien de bron YouForce is dan moet voor elk personeelsnummer binnen IAM een IAM-account aangemaakt worden. Dus elk personeelsnummer resulteert in een unieke TOPdeskpersoonskaart. Medewerkers die direct IAM ingevoerd worden hebben geen personeelsnummer maar wel een IAM-account. Voor deze IAM-accounts moet ook een TOPdeskpersoonskaart aangemaakt worden.

Veldnaam	Omschrijving	Type	Gekoppelde tabel	Bron
Key velden				
Sleutel_IAM_account	Unieke sleutel van de IAM-persoonskaart	Nummeriek		IAM
Persoon.personeelsnr	Personeelsnummer uit YouForce. Indien medewerkings direct ingevoerd zijn in IAM dan is dit veld leeg.	Tekst		YOUFORCE
Container	Zaanstad, SWT, JT of externe account			
Attributen op persoonskaart				
Persoon.achternaam	Achternaam	Tekst		YOUFORCE, Form*
Persoon.voornaam	Voornaam	Tekst		YOUFORCE, Form*
Persoon.voorletters	Voorletters	Tekst		YOUFORCE, Form*
Persoon.ref_dynanaam	Samengestelde naam (achternaam, voornaam voorvoegsel)	Type		YOUFORCE, Form*
Persoon.geslacht	Geslacht	Integer (1=man, 2=vrouw)		YOUFORCE, Form*
Persoon.email	E-mail	Tekst		AD
Persoon.extraapersoonid	Organisatieonderdeel	Unid	Extraapersoon	Zie paragraaf hierna
Persoon.extrabpersoonid	Afdeling (***)	Unid	Extrabpersoon	Zie paragraaf hierna
Persoon.afdelingid	Team (***)	Unid	Afdeling	Zie paragraaf hierna
Persoon.functie	Functie (werknaam)	Tekst		YOUFORCE, Form*
Persoon.vrijetekst1	Hr21-functie	Tekst		YOUFORCE, Form*
Persoon.loginnaamnetwerk	Inlognaam netwerk (SAM account)	Tekst		AD
Persoon.tasloginnaam	Inlognaam SSP (SAM account)	Tekst		AD
Persoon.vestigingid	Locatie (**)	Unid	Vestiging	IAM
Persoon.lokatieid	Ruimte	Unid	Locatie	nvt
Persoon.managerid	Manager	Unid	Persoon	YOUFORCE, Form*
Persoon.ismanager	Is manager (ja/nee) (*)	Logisch		YOUFORCE, Form*

Persoon.hire_date	Datum indiensttreding	Datum		YOUFORCE, Form*
Persoon.service_date	Datum uitdiensttreding	Datum		YOUFORCE, Form*
Persoon.dataanmk	Datum aanmaak	Datum		IAM
Persoon.datwijzig	Datum wijziging	Datum		IAM
Persoon.uidaanmk	Aanmaker van de kaart (=IAM, IAM)	Unid	Gebruiker	IAM
Persoon.uidwijzig	Wijziger van de kaart (=IAM, IAM)	Unid	Gebruiker	IAM
Persoon.status	Archief	Integer (1 = Actief, -1 = Gearchiveerd)		IAM
Persoon.archiefredenid	Archiefreden (persoon uit dienst)	Unid	Archiefreden	IAM
Persoon. budgethouderid	Kostenplaats	Unid	Budgethouder	IAM
Persoon.telefoon	Telefoonnummer	Tekst		Handmatig
Persoon.mobiel	Mobiel nummer	Tekst		Handmatig

(*) Het logische veld persoon.ismanager moet worden aangevinkt wanneer de medewerker als SLG is ingesteld bij de desbetreffende organisatie-eenheid in het personeelssysteem.
(**) Bij het veld locatie worden standaard de volgende waardes ingevuld afhankelijk van de identiteit/arbeidsrelatie:
(***) Als een medewerker naar een hogere organisatie-eenheid gaat dan kan het voorkomen dat de medewerker geen team (en zelfs geen afdeling) meer heeft. Deze gegevens moeten dan gewist worden op de persoonskaart.

*Dertig dagen na de datum van uitdiensttreding wordt het AD-account verwijderd. Op dat moment worden in TOPdesk de velden **persoon.tasloginnaam** en **persoon.loginnaamnetwerk** geleegd en wordt de TOPdesk-persoonskaart gearchiveerd.*

Arbeidsrelatie	**Waarde Locatie**
BML-01, BML-10, BML-15, BML-20, BML-25, BML-30, BML-50, BML-52, BML-53, BML-54, BML-55, BML-56, BML-57, BML-58, BML-59, BML-60, BML-70, BML-87, BML-88, BML-89, BML-93, BML-94	Stadhuis
BML-90	SWT
BML-91	JT

Stamtabellen organisatie-eenheden en leidinggevenden

Bij het aanmaken van persoonskaarten in TOPdesk moet rekening gehouden worden met het feit dat medewerkers ontstaan vanuit 2 bronnen:

- YouForce
- Directe invoer van medewerkers in de IAM-applicatie

Medewerkers vanuit YouForce hebben in hun dienstverband een organisatie-eenheid. De relevante organisatie-eenheden en de bijbehorende leidinggevenden moeten door de Oplossing worden verwerkt in een beheersbare organisatiestructuur.

In TOPdesk worden per organisatie-eenheid maximaal drie organisatieniveaus gebruikt: organisatieonderdeel, afdeling en team. In YouForce kunnen meer niveaus aanwezig zijn. De Oplossing moet de onderliggende structuur en relaties tussen de organisatie-eenheden vertalen naar de drie TOPdesk-niveaus.

Opdrachtgever schrijft hiervoor geen specifieke realisatievorm voor. De vertaling mag worden gerealiseerd door middel van een script, csv-import, frontend-invoer of een andere passende inrichting, mits de gewenste en beheersbare vertaling naar de TOPdesk-structuur wordt gerealiseerd.

Ook organisatie-eenheden en leidinggevenden voor handmatig ingevoerde identiteiten moeten beheersbaar kunnen worden vastgelegd. Bij het invoeren van een identiteit moet de relevante organisatie-eenheid selecteerbaar zijn, waarna de bijbehorende leidinggevende, het organisatieonderdeel, de afdeling en het team kunnen worden bepaald.

Wij zien 2 opties:

- Of een csv bestand
- Of invoeren via de frontend

Usecase	Organisatie Eenheid (A)	Leidinggevende bij OE (B)	Organisatie Onderdeel (C)	Afdeling (D)	Team (E)	IAM ja/nee (*)
YOUFORCE						
Nieuw OE	Script voegt nieuwe waarde toe in OE-tabel					
Create/update LG bij OE		Script voegt LG toe bij OE-tabel				
Organisatieonderdeel bij OE (level1)			Óf complex script Óf csv Óf frontend			
Afdeling bij OE (level2)				Óf complex script Óf csv Óf frontend		
Team bij OE (level3)					Óf complex script Óf csv Óf frontend	
IAM ja/nee (*)						Óf script Óf csv Óf frontend
SWT, JT en externe accounts						
Nieuwe OE	óf front-end óf csv mergen (**)					
Create/update LG bij OE		Óf csv Óf front-end				
Organisatieonderdeel bij OE			Óf csv Óf frontend			
Afdeling bij OE				Óf csv Óf frontend		

Team bij OE					Óf csv Óf frontend	

(*) In YouForce zitten een aantal organisatie-eenheden die buiten IAM moeten vallen. Bijvoorbeeld wachtgelders. Hiervoor zijn 3 opties
(**) Er wordt gesproken over mergen omdat de organisatie-eenheden in dezelfde tabel komen als de organisatie-eenheden uit YouForce.

Figuur 1 – organisatie-eenheid in dienstverband van medewerker

```
<dienstverband>
<identificatieDV>
 <persNrDV>4360</persNrDV>
 <dvVlgnr>1</dvVlgnr>
</identificatieDV>
<periodeDV>
<begindatum>
 <rubriekcode>P00322</rubriekcode>
 <datumIngang>2016-09-01</datumIngang>
 <omschrijvingRubriek>Datum in dienst</omschrijvingRubriek>
 <omschrijvingWaarde/>
 <waarde>1989-05-08</waarde>
</begindatum>
<einddatum>
 <rubriekcode>P00830</rubriekcode>
 <datumIngang>1989-05-08</datumIngang>
 <omschrijvingRubriek>Datum uit dienst</omschrijvingRubriek>
 <omschrijvingWaarde/>
 <waarde/>
</einddatum>
</periodeDV>
<arbeidsRelatie>
<volgnrDienstverband>
 <rubriekcode>P01101</rubriekcode>
 <datumIngang>2016-09-01</datumIngang>
 <omschrijvingRubriek>Volgnr dienstverband</omschrijvingRubriek>
 <omschrijvingWaarde/>
 <waarde>1</waarde>
</volgnrDienstverband>
<opdrachtgeverNr>
 <rubriekcode>P01103</rubriekcode>
 <datumIngang>2016-09-01</datumIngang>
 <omschrijvingRubriek>Opdrachtgever</omschrijvingRubriek>
 <omschrijvingWaarde>Gemeente Zaanstad</omschrijvingWaarde>
 <waarde>23356</waarde>
</opdrachtgeverNr>
<orgEenheid>
 <rubriekcode>P01106</rubriekcode>
 <datumIngang>2025-06-01</datumIngang>
 <omschrijvingRubriek>Organisatorische een</omschrijvingRubriek>
 <omschrijvingWaarde>3933</omschrijvingWaarde>
 <waarde>644</waarde>
</orgEenheid>
<soortArbeidsrelatie>
```

XML-roltoewijzing

Figuur 2 Voorbeeld roltoewijzing (dus leidinggevende bij organisatie-eenheid)

ns1:datumTijd	ns1:klantID	ns1:klantCode	ns1:klantNaam	ns1:functieCode	ns1:functieOmschrijving
2026-01-06 18:17:37	4024838	4024838		21090	Trainee
2026-01-06 18:17:37	4024838	4024838		22000	Medewerker Algemene dienst
2026-01-06 18:17:37	4024838	4024838		23000	Medewerker Leerwerktraject
2026-01-06 18:17:37	4024838	4024838		24000	Medewerker Externe inhuur
2026-01-06 18:17:37	4024838	4024838		25000	Stagiair
2026-01-06 18:17:37	4024838	4024838		26000	ZZP
2026-01-06 18:17:37	4024838	4024838		27000	Fractieassistent
2026-01-06 18:17:37	4024838	4024838		1	Medewerker technische uitvoering IV
2026-01-06 18:17:37	4024838	4024838		10	Medewerker ontwerp & voorbereiding V
2026-01-06 18:17:37	4024838	4024838		11	Medewerker beleidsuitvoering III
2026-01-06 18:17:37	4024838	4024838		1102160	Griffier I
2026-01-06 18:17:37	4024838	4024838		1104140	Griffier II
2026-01-06 18:17:37	4024838	4024838		12	Medewerker beleidsuitvoering II
2026-01-06 18:17:37	4024838	4024838		14	Operationeel leidinggevende IV
2026-01-06 18:17:37	4024838	4024838		15	Medewerker bedrijfsvoering I
2026-01-06 18:17:37	4024838	4024838		16	Medewerker beleidsuitvoering I
2026-01-06 18:17:37	4024838	4024838		17	Medewerker ontwerp & voorbereiding III
2026-01-06 18:17:37	4024838	4024838		18	Adviseur IV
2026-01-06 18:17:37	4024838	4024838		19	Operationeel leidinggevende III
2026-01-06 18:17:37	4024838	4024838		2	Medewerker technische uitvoering II
2026-01-06 18:17:37	4024838	4024838		20	Medewerker beleidsuitvoering 0
2026-01-06 18:17:37	4024838	4024838		21	Adviseur III
2026-01-06 18:17:37	4024838	4024838		2102180	Gemeente secretaris / algemeen directeur
2026-01-06 18:17:37	4024838	4024838		2104170	Directeur I
2026-01-06 18:17:37	4024838	4024838		2106160	Directeur II
2026-01-06 18:17:37	4024838	4024838		22	Adviseur II
2026-01-06 18:17:37	4024838	4024838		2202150	Strategisch manager I
2026-01-06 18:17:37	4024838	4024838		2204140	Strategisch manager II
2026-01-06 18:17:37	4024838	4024838		23	Tactisch leidinggevende II
2026-01-06 18:17:37	4024838	4024838		2302140	Manager I
2026-01-06 18:17:37	4024838	4024838		2304130	Manager II
2026-01-06 18:17:37	4024838	4024838		2306120	Manager III
2026-01-06 18:17:37	4024838	4024838		24	Manager III
2026-01-06 18:17:37	4024838	4024838		2404120	Tactisch leidinggevende II
2026-01-06 18:17:37	4024838	4024838		2406110	Tactisch leidinggevende III
2026-01-06 18:17:37	4024838	4024838		25	Projectleider II
2026-01-06 18:17:37	4024838	4024838		2502110	Operationeel leidinggevende I
2026-01-06 18:17:37	4024838	4024838		2504550	Operationeel leidinggevende II
2026-01-06 18:17:37	4024838	4024838		2506100	Operationeel leidinggevende III
2026-01-06 18:17:37	4024838	4024838		2508090	Operationeel leidinggevende IV
2026-01-06 18:17:37	4024838	4024838		2510080	Operationeel leidinggevende V
2026-01-06 18:17:37	4024838	4024838		26	Programmamanager II (tijdelijke formatie)
2026-01-06 18:17:37	4024838	4024838		2600150	Programmamanager IA
2026-01-06 18:17:37	4024838	4024838		2602140	Programmamanager I
2026-01-06 18:17:37	4024838	4024838		2604130	Programmamanager II
2026-01-06 18:17:37	4024838	4024838		2606120	Programmamanager III
2026-01-06 18:17:37	4024838	4024838		27	Manager II

Indicatieve vertaling organisatiehiërarchie

De onderstaande vertaalregels, nummerreeksen, uitzonderingen en voorbeelden beschrijven de huidige situatie en zijn uitsluitend illustratief. Zij vormen geen volledige of uitputtende set implementatieregels. De organisatiehiërarchie moet primair worden afgeleid uit de onderliggende structuur en de relaties tussen de organisatie-eenheden.

V.w.b het vullen van de organisatie-eenheden onderkennen we 3 niveaus in TOPdesk, terwijl dit er in het personeelssysteem een stuk of 5 zijn. Daarom moet er in de koppeling een vertaalslag worden uitgevoerd om de juiste organisatie-eenheden in de de TOPdesk-velden te verkrijgen. In TOPdesk hanteren we de niveaus Organisatieonderdeel, Afdeling en Team.

De plaatsing van organisatie-eenheden in de TOPdesk-velden organisatieonderdeel, afdeling en team wordt bepaald op basis van de onderlinge hiërarchische relaties. De lengte van de korte code kan daarbij ondersteunende informatie geven, maar is niet zelfstandig of in alle gevallen bepalend.
In de huidige structuur geldt in hoofdlijnen:

- een cluster bestaat uit twee posities;
- afdelingen vallen onder een cluster en kunnen door drie of vier posities worden aangeduid;
- teams vallen onder een afdeling en kunnen daardoor door vier of vijf posities worden aangeduid.

Afwijkingen en uitzonderingen kunnen voorkomen. De onderstaande tabel bevat voorbeelden van de huidige situatie.

Uitzondering hierop is de organisatie-eenheid ‘Directie’, hiervan heeft de korte code een lengte van 1 maar dient gebruikt te worden als organisatie-onderdeel wanneer de medewerker orgEenheidId 180 heeft.

Als een medewerker een orgEenheidId heeft van 180 of een waarde tussen 184 t/m 564 dan moet in TOPdesk alleen het veld ‘Organisatieonderdeel’ voorzien worden van de organisatie-eenheid, en moeten de andere velden ‘Afdeling’ en ‘Team’ leeg blijven.

In onderstaande voorbeelden wordt weergegeven welke waarden de TOPdesk-velden moeten krijgen a.d.h.v. de desbetreffende orgEenheidId en korte code.

Medewerker bevat orgEenheidId	**Korte Code**	**Organisatieonderdeel**	**Afdeling**	**Team**
180	1	Directie	[LEEG]	[LEEG]
186	93	Burgemeester	[LEEG]	[LEEG]
315	11	Raadsgriffie	[LEEG]	[LEEG]
546	98	Raadsleden	[LEEG]	[LEEG]
569	40	Control	[LEEG]	[LEEG]
568	39	Cluster Bedrijfsvoering	[LEEG]	[LEEG]
613	399	Cluster Bedrijfsvoering	Business Control	[LEEG]
607	393	Cluster Bedrijfsvoering	IBT	[LEEG]
644	3933	Cluster Bedrijfsvoering	IBT	Functioneel Beheer
566	37	Cluster Collectieve Dienstverlening	[LEEG]	[LEEG]
584	373	Cluster Collectieve Dienstverlening	Straattoezicht	[LEEG]
688	3733	Cluster Collectieve Dienstverlening	Straattoezicht	Straattoezicht Uitvoering

689	37331	Cluster Collectieve Dienstverlening	Straattoezicht	Straattoezicht Uitvoering

In de korte code van organisatie-eenheden met een korte code-lengte van 2 of hoger kunnen de bovenliggende niveau's worden bepaald door de laatste cijfer(s) weg te laten.

Een korte code met meer dan vier posities betekent niet automatisch dat de organisatie-eenheid buiten TOPdesk blijft. De juiste registratie in TOPdesk wordt bepaald op basis van de onderliggende hiërarchie en de gewenste vertaling naar organisatieonderdeel, afdeling en team.

Bij deze medewerkers worden dan alleen de hogere niveaus gehanteerd. In bovenstaande tabel is dit te zien bij de orgEenheidId 688 en 689. In TOPdesk krijgen ze in dat geval de waarden van het hogere organisatieniveau.

Registratie organisatie-eenheden tbv medewerkers die niet in het personeelssysteem staan

Dit betreft de registratie t.b.v. organisatie-eenheden van medewerkers die (nu nog) handmatig via formulieren in IAM worden geregistreerd, en vooralsnog niet worden beheerd in het personeelssysteem. De organisatie-eenheden en leidinggevenden hiervan worden beheerd in een aparte .csv tabel, welke selecteerbaar zijn in hetzelfde dropdown-veld dat gebruikt wordt voor de organisatie-eenheden van het personeelssysteem. Dit .csv bestand is als volgt samengesteld:

Korte naam organisatie-eenheid;Lange naam organisatie-eenheid;Beschrijving;Userid van leidinggevende;TOPdesk Unid van Leidinggevende

Voorbeeld

short_name;long_name;description;manager_userid;manager_unid_TOPdesk
ow_swt01;SWT01;SWT01 Krommenie;BAA1L;03FE074B-1706-4D41-A88F-1EBEA0A27506
ow_swt02;SWT02;SWT02 Wormerveer;SCH1S;c5faf7d5-38ad-4abc-95cd-0a89c59f1f61
ow_swt03;SWT03;SWT03 Assendelft - Westzaan;KRIJM;4dc1d920-6e39-45c9-bd63-0320d48321e7
ow_swt04;SWT04;SWT04 Oud Koog - Oud Zaandijk;ELDEM;3c825ca3-5406-4f5a-a69e-8732a4042624
ow_swt05;SWT05;SWT05 Zaandam Noord - Kogerveld;DEJOM;a8487a82-37cb-4a08-8f66-efa7566df8c8
ow_swt06;SWT06;SWT06 Zaandam Nieuw West / Westerkoog / Rooswijk;MUTSS;45bf9808-7a73-51e6-9e6a-62e7b5acc271
ow_swt07;SWT07;SWT07 Peldersveld - Hoornseveld;HANST;68dc549b-0306-5148-937b-227b40c5f3e8
ow_swt08;SWT08;SWT08 Zaandam West - Oude Haven;MACHD;b3bdef19-a6fe-4182-8cc5-156da30647fd
ow_swt09;SWT09;SWT09 Rosmolenwijk;BEEKS;8951563b-bd94-4e08-9ad8-10342dfb20ab
ow_swt10;SWT10;SWT10 Poelenburg;BEZEA;38c95766-7bac-4b71-8286-dd325117e8ce
ow_swt11;SWT11;SWT11 Zaandam Zuid;BOUJM;31d077cd-00fd-4538-bb14-63fac86eb2d1

ow_jt00;JT00;JT00 Zaandam Zuid - Hoofdkantoor SJZ;BOR1P;6D6D7BF1-6289-43FD-BBE0-072DC8DED993
ow_jt01;JT01;JT01 Krommenie/Wormerveer;assol;764eddf4-e552-48fb-830b-158de889473a

ow_jt02;JT02;JT02 Nieuw West, Oud Koog, Oud Zaandijk, Rooswijk, Westerkoog;KOP2M;6EBC1619-DA39-49D6-9265-E7371B1D2BA4
ow_jt03;JT03;JT03 Kogerveld, Zaandam Noord, Zaandam West, Oude Haven;BEUKM;12B34FFA-9509-556D-9A7C-3DDF2E34AFFF
ow_jt04;JT04;JT04 Rosmolenwijk, Zaandam Zuid;KOP2M;6EBC1619-DA39-49D6-9265-E7371B1D2BA4
ow_jt05;JT05;JT05 Pelders- en Hoornseveld, Poelenburg;BEUKM;12B34FFA-9509-556D-9A7C-3DDF2E34AFFF
ow_jt06;JT06;JT06 Assendelft/Westzaan;assol;764eddf4-e552-48fb-830b-158de889473a
ou_wormerland;Overgemeente;Overgemeente;STEBK;1741b9d6-89b1-511e-b66b-d14b5a33400a
ou_werkom;Werkom;Werkom;STEBK;1741b9d6-89b1-511e-b66b-d14b5a33400a
ou_omgevingsdienst;Omgevingsdienst;Omgevingsdienst;KROEA;3e5b7464-e38c-5ac4-b492-b83dde59dac2
ou_lev_iens;Leveranciers I&S; Leveranciers I&S;DOVEG;7801cc4f-46d6-5462-a0e1-486445ef1a3c

Dit moet leiden tot een registratie van organisatie-eenheden bij de medewerkers in TOPdesk op de volgende manier:

Korte Code	Organisatieonderdeel	Afdeling	Team
ow_swt01	Sociaal Wijkteam	SWT 01 Krommenie	[LEEG]
ow_swt02	Sociaal Wijkteam	SWT 02 Wormerveer	[LEEG]
ow_swt03	Sociaal Wijkteam	SWT 03 Assendelft-Westzaan	[LEEG]
ow_swt04	Sociaal Wijkteam	SWT 04 Oud Koog-Oud Zaandijk	[LEEG]
ow_swt05	Sociaal Wijkteam	SWT 05 Zaandam Noord-Kogerveld	[LEEG]
ow_swt06	Sociaal Wijkteam	SWT 06 Zaandam Nieuw West / Westerkoog / Rooswijk	[LEEG]
ow_swt07	Sociaal Wijkteam	SWT 07 Peldersveld-Hoornseveld	[LEEG]
ow_swt08	Sociaal Wijkteam	SWT 08 Zaandam West-Oude Haven	[LEEG]
ow_swt09	Sociaal Wijkteam	SWT 09 Rosmolenwijk	[LEEG]
ow_swt10	Sociaal Wijkteam	SWT 10 Poelenburg	[LEEG]
ow_swt11	Sociaal Wijkteam	SWT 11 Zaandam Zuid	[LEEG]
ow_jt00	Jeugdteam	JT 00	[LEEG]
ow_jt01	Jeugdteam	JT 01	[LEEG]
ow_jt02	Jeugdteam	JT 02	[LEEG]
ow_jt03	Jeugdteam	JT 03	[LEEG]
ow_jt04	Jeugdteam	JT 04	[LEEG]
ow_jt05	Jeugdteam	JT 05	[LEEG]
ow_jt06	Jeugdteam	JT 06	[LEEG]
ou_werkom	Extern	Werkom	[LEEG]
ou_wormerland	Extern	Overgemeente	[LEEG]
ou_omgevingsdienst	Extern	Omgevingsdienst	[LEEG]
ou_lev_iens	Extern	Leveranciers I&S	[LEEG]

Ook hier geldt dat het leidinggevende vinkje moet worden aangezet in persoon.ismanager bij leidinggevenden.

Koppeling TOPdesk -> IAM

Van TOPdesk moet slechts de velden persoon.telefoon en persoon.mobiel worden overgenomen in de persoonskaart in IAM.

Uitsluiting

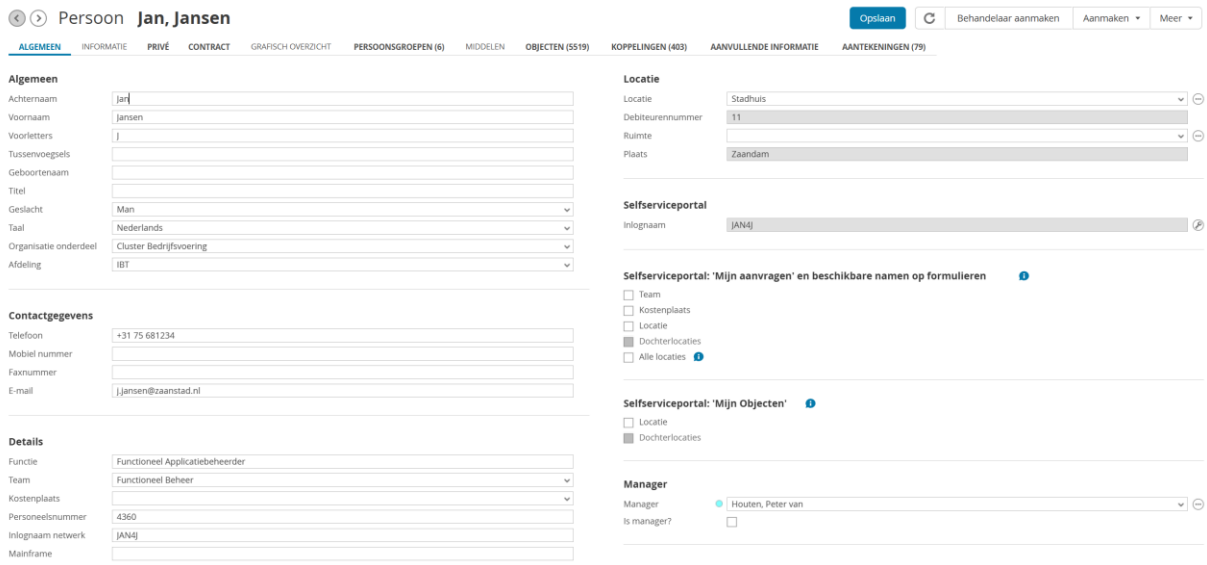
Medewerkers die onderstaande organisatie-eenheden bevatten, worden niet meegenomen in de koppeling:

- 178 Speciale functies
- 179 Algemeen raadsgriffie
- 188 Voormalig bestuurders
- 190 Wachtgelders
- 477 Test directie
- 478 Test domein

- 479 Test sector
- 480 Test afdeling I
- 481 Test afdeling II

Tenslotte
Voordat de organisatiegegevens op een TOPdesk-persoonskaart worden gewijzigd, moeten de bestaande velden voor organisatieonderdeel, afdeling en team eerst worden geleegd en vervolgens met de nieuwe, van toepassing zijnde waarden worden gevuld. Hiermee wordt voorkomen dat bij verplaatsing naar een hoger organisatieniveau oude gegevens voor afdeling of team op de persoonskaart blijven staan. Dit verzoek zou ervoor moeten zorgen dat wanneer een medewerker wordt verplaatst naar een hoger organisatie-niveau, de afdeling en team blijven staan waar dat niet meer van toepassing is.

Voorbeeld persoonskaart in TOPdesk



Voorbeeld BINT-bestand uit personeelssysteem met organisatie-eenheden

orgEenheidID	korte Code	Naam organisatieeenheid	hogereOrgEenheid
1	HOE	Gemeente Zaanstad	
178	9	Speciale functies	1
179	1	Algemeen Raadsgriffie	1
180	2	Directie	1
477	7	Test directie	1
184	91	Raadsleden	178
185	92	Steunfractieleden	178
186	93	Burgemeester	178
187	94	Wethouders	178
188	95	Voormalig bestuurders	178
189	96	Bijzondere ambtenaren Burgelijke Stand	178
190	97	Wachtgelders c.a.	178
546	98	Fractieassistenten	178
315	11	Raadsgriffie	179
553	24	Gebied Noord	180
554	25	Gebied Midden	180

555	26	Gebied Oost	180
556	27	Gebied Buiten	180
557	28	Gebied Noordzeekanaal	180
558	29	Opgave Economie	180
559	30	Opgave Kansengelijkheid	180
560	31	Opgave Gezondheid	180
561	32	Opgave Duurzaamheid	180
562	33	Opgave Verstedelijking	180
563	34	Opgave Veiligheid	180
564	35	Opgave Samenwerken aan Zaanstad	180
565	36	Cluster Individuele Dienstverlening	180
566	37	Cluster Collectieve Dienstverlening	180
567	38	Cluster Strategie en Beleid	180
568	39	Cluster Bedrijfsvoering	180
569	40	Control	180
675	41	Programmabureau Pact Zaandam Oost	180
478	71	Test domein	477
479	711	Test sector	478
480	7111	Test Afdeling I	479
481	7112	Test Afdeling II	479
482	71111	Test Team Afdeling I	481
483	71121	Test Team Afdeling II	481
529	236121	Receptie (tbv Roosterplanning)	528
570	361	Callcenter	565
571	362	Burgerzaken	565
572	363	Belastingen	565
573	364	Gemeentearchief	565
574	365	Bouw RO	565
575	366	Omgevingsvergunningen	565
576	367	Voorzieningen	565
577	368	Uitkeringen	565
578	369	Jongerenloket	565
579	3610	Naleving	565
580	3611	Stedelijke Toegang	565
581	3612	Juridische Zaken	565
582	371	Relatie en Wijkmanagement	566
583	372	Projecten	566
584	373	Straattoezicht	566
586	375	Aanpak Ondermijning	566
587	376	Havens en Vaarwegen	566
588	377	Gebiedsontwikkeling	566
589	378	Wijkbeheer en Onderhoud	566
590	379	Stadsbeheer en Onderhoud	566
591	3710	Ingenieursbureau	566
592	3711	Strategie en Beleid	566
593	3712	Projectmanagement	566
594	3713	Grondzaken	566
595	381	Openbare Orde & Veiligheid	567
596	382	Fysieke Leefomgeving I	567
597	383	Fysieke Leefomgeving II	567
598	384	Omgevingsplannen	567
599	385	Stedelijke Kaders en Regie	567
600	386	Kennis	567

601	387	Contractmanagement	567
602	388	Strategie en Onderzoek	567
603	389	Frontlijn	567
678	3811	Programmamanagement en Opgaveregie	567
605	391	P&O	568
606	392	Inkoop en Subsidies	568
607	393	IBT	568
608	394	Facilitaire Zaken	568
609	395	Bestuur- en Managementondersteuning	568
610	396	Communicatie	568
611	397	DIV	568
612	398	Financiën	568
613	399	Business Control	568
614	401	Kaders Regie en Auditing	569
615	3621	GBS/Kwaliteit	571
616	3622	DVL/Receptie	571
686	3631	Team Heffen en Invorderen	572
687	3632	Team Taxateurs / Gegevensbeheer / Geo	572
679	3651	Team Beleid & Advies Bouw RO	574
680	3652	Team Toezicht Bouw RO	574
667	3671	Team Leerlingenvervoer	576
668	3672	Team Voorzieningen WMO / Jeugd	576
669	3673	Team Minima	576
661	3681	Team Uitkeringsadm. en Financiële adm.	577
662	3682	Team Terugvordering en Ondersteuning	577
663	3683	Team Casemanagement en Procesbeheer	577
617	3691	Straathoekwerk	578
673	3692	Leerplicht	578
664	36101	Team Taskforce Werk of Meedoen	579
665	36102	Team PW Regulier	579
666	36103	Team Naleving WMO / Jeugd	579
656	36111	Gemeentelijk Team Inburgering	580
681	36112	Team KOT Stedelijke Toegang	580
618	36121	Juridisch advies/bezwaar en beroep	581
619	36122	Secretariaat bezwaar en beroep	581
620	36123	Schade en Verzekeringen	581
688	3733	Straattoezicht Uitvoering	584
625	3761	Havenbeambten	587
626	3762	Operators	587
627	3781	Team Onderhoud	589
628	3782	Team Beheer	589
629	3783	Team Ondersteuning	589
630	3784	Team Arbeidsparticipatie	589
631	3785	Team Afval en Reiniging	589
674	3786	Team Super Snel Schoon	589
632	3791	Team Riool	590
633	3792	Team Infra	590
634	3793	Team Groen en Water	590
635	37101	Team Projectleiding	591
636	37102	Team Strategisch Advies	591
637	37103	Team Voorbereiding	591
657	37104	Team Uitvoering en Bouwkunde	591
670	37105	Team Ondergrondse Infra	591

671	37106	Team IB Ondersteuning	591
672	37107	Team Grote Projecten	591
638	37111	Team Strategie en Programmering	592
639	37112	Team Bestands- en Informatiebeheer	592
682	3831	Team Erfgoed	597
683	3832	Team Milieu	597
684	3833	Team Ecologie	597
685	3834	Team Ontwerpers Openbare Ruimte	597
677	3861	Team Welzijn	600
676	3891	Team Zorg en Veiligheidshuis	603
640	3911	Team P&O Advies Beleid & Recruitment	605
643	3932	Informatie- Proces- en Projectmanagement	607
644	3933	Functioneel Beheer	607
645	3934	Infrastructuur en Support	607
659	3935	Servicedesk en Changemanagement	607
660	3936	Procesmanagement en Functioneel Beheer 2	607
646	3951	Team BMO	609
648	3953	Team Managementsecretariaat	609
650	3961	Woordvoering	610
651	3962	Advies en Redactie	610
658	3963	Kabinet en Bestuurssecretariaat	610
652	3981	Financieel Adviseurs	612
653	3982	Financieel Specialisten	612
654	3983	Financieel Beheer	612
655	3984	Financieel Transacties	612
694	36211	BZ Urgenties	615
695	36212	BZ GBS & Kwaliteit	615
696	36221	BZ DVL	616
697	36222	BZ Receptie	616
698	36223	BZ Adreskwaliteit	616
689	37331	Team APV Straattoezicht	688
690	37332	Team Parkeren Straattoezicht	688
691	37333	Team TWO Straattoezicht	688
692	37334	Team Juristen Straattoezicht	688
693	37335	Team Administratie Straattoezicht	688