Vlaams Gebruikers- en Toegangsbeheer

Integreren kun je leren

DIGITAAL VLAANDEREN

Vlaamse overheid

Inhoudsopgave

Introductie

Deze presentatie:

- Bevat praktische informatie over de **verschillende keuzes** die aan bod kunnen komen tijdens een integratietraject van uw toepassing op het Vlaams Gebruikers- en Toegangsbeheer (IDM/ACM)

- Veronderstelt basiskennis van de bouwstenen en terminologie
  - Zie op onze website ook onze kennismakingspresentatie en het integratieproces

- Helpt u om samen met het integratieteam een optimale aansluiting te realiseren
  - Een gedegen analyse van uw noden en behoeften samen met het integratieteam is altijd leidend; begin niet vanuit het integratiedossier of de mogelijke en geboden opties, maar altijd vanuit uw eigen noden en behoeften!

Werken volgens open standaarden

- Het Gebruikers- en Toegangsbeheer werkt volgens open standaarden, zodat we maximaal en toekomstgericht kunnen ontsluiten
  - We bieden een standaard integratietraject aan op basis van standaardcomponenten waardoor de doorlooptijden en technische opzet transparant zijn voor eindgebruikers/klanten

- De standaard aanpak zorgt voor een zo kort mogelijke doorlooptijd, kosteloze integraties voor de afnemer, en zo beperkt mogelijke complexiteit

- Vooral de eindgebruikers profiteren van rechtlijnigheid en stabiliteit in de integraties

Standaard versus niet-standaard traject

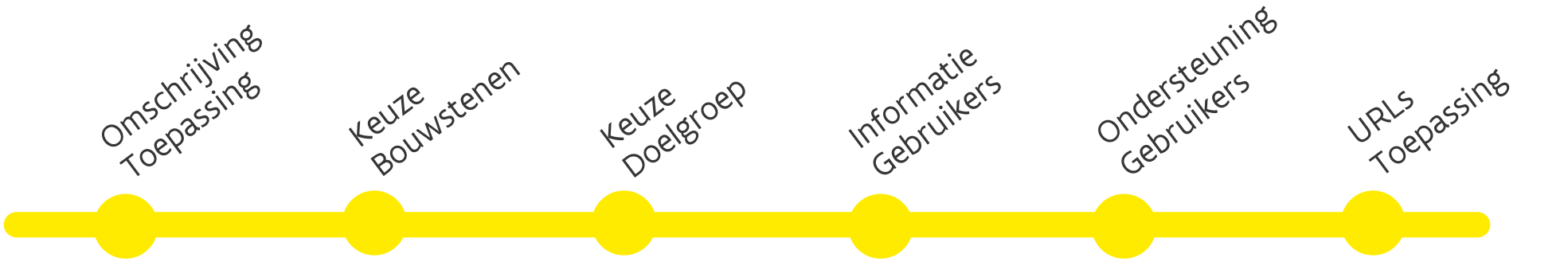
- De standaard dekt ruim 95% van de aanvragen af, maar ook buiten de standaard helpen we u graag verder (op basis van offertekost)
  - Standaard
    - Claims based authenticatie (SAML 2.0, OpenID Connect, Reverse Proxy)
    - Gedelegeerd beheer van gebruikers- en rechten via de online toepassing
    - Informatie in standaard formaten
  - Niet standaard
    - Provisionering van gebruikers- en rechteninformatie via webservices
    - Dynamisch ophalen van rechteninformatie door IDM (EAWS)
    - Nieuwe functionaliteiten en overig maatwerk

1. Algemene keuzes en benodigde informatie

DIGITAAL VLAANDEREN

Vlaamse overheid

Belangrijkste onderwerpen



DIGITAAL VLAANDEREN

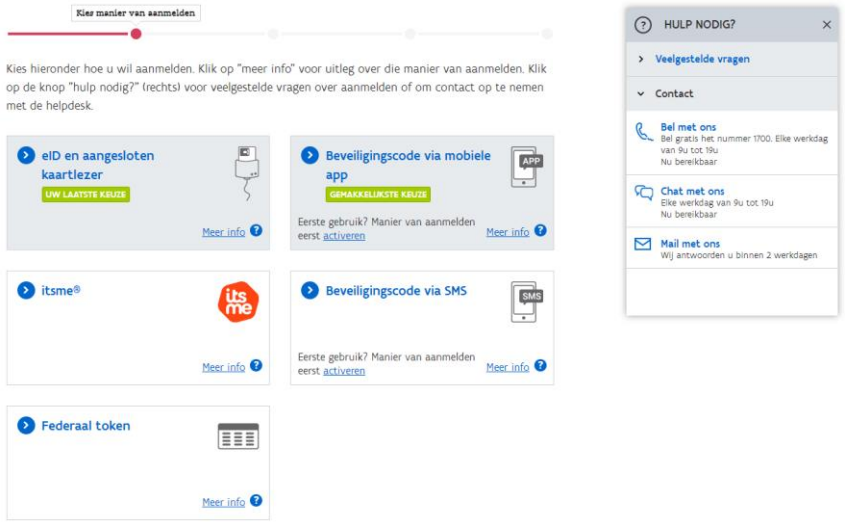
Vlaamse overheid

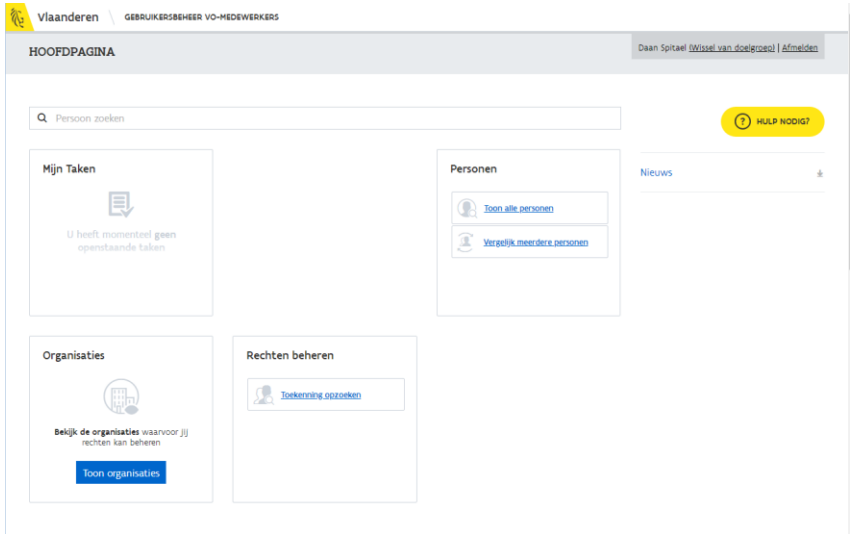
Vertel! Omschrijving van je toepassing

- Wat doet de toepassing?
  - En wat kunnen gebruikers? Wie zijn de verschillende typen gebruikers?
    - Bijvoorbeeld, een eLoket op een gemeentelijke website waar burgers en bedrijven start-up subsidies kunnen aanvragen, die vervolgens door medewerkers van de gemeente goedgekeurd kunnen worden.

- Een goede inhoudelijke beschrijving van de toepassing helpt niet alleen een juiste analyse te maken voor het integratiescenario, maar kan onze ondersteuners later ook helpen om gebruikers effectief te woord te staan
  - Wat werkt voor grote organisaties als een departement van de Vlaamse Overheid, werkt niet altijd voor kleine ondernemers of burgers; het integratieteam denkt graag mee voor de juiste implementatie.

Welke bouwstenen?





ACM: Toegangsbeheer

- Toegang krijgen
  - → Aanmelden
  - → Identificeren
  - → Authenticeren

IDM: Gebruikersbeheer

- Toegang geven
  - → Gebruikers beheren
  - → Rechten beheren

DIGITAAL VLAANDEREN

Vlaamse overheid

Keuze Bouwstenen

Welke bouwstenen?

- Het Toegangsbeheer (ACM) en het Gebruikersbeheer (IDM) kunnen samen of afzonderlijk worden afgenomen.

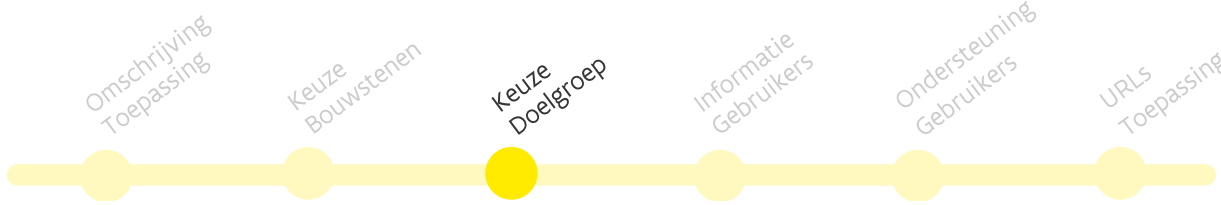
- ACM en IDM
  - ACM identificeert en authenticeert gebruikers, beheert toegang grofmazig op beheer van rechten in IDM, en levert gebruikersinformatie mee zoals gekend in IDM (e.g. fijnmazige rollen)
- Enkel ACM
  - Wanneer alleen vraag naar identificatie en authenticatie, geen gebruikers- of rechtenbeheer (indien nog rechtenbeheer in de toepassing, te heroverwegen)
  - Bijvoorbeeld wanneer de toepassing enkel beschikbaar is voor burgers
- Enkel IDM
  - Wanneer de toepassing zelf identificatie en authenticatie afhandelt, en IDM gebruikt wordt voor beheer van gebruikers en hun rechten. Niet gebruikelijk (of aan te raden)

Voor wie? Doelgroepen

- Het Vlaams Gebruikers- en Toegangsbeheer kan gebruikt worden zowel voor:
  - **Interne** medewerkers (‘back-office’ van overheden)
  - **Externe** doelgroepen (‘front-office’; burgers, medewerkers van organisaties)

- We onderscheiden de volgende doelgroepen:
  - Burgers (als particulier, dus ‘namens’ zichzelf): “BUR”
  - Entiteiten van de Vlaamse Overheid (departementen, agentschappen): “GID”
  - Lokale Besturen (provincies, steden, gemeenten, politiezones, etc.): “LB”
  - Onderwijs- en Vormingsinstellingen (scholen, universiteiten, CLB’s, etc.): “OV”
  - Bedrijven en andere organisaties (organisaties met een KBO-nummer): “EA”

- Subsets van organisaties zijn ook mogelijk binnen de doelgroepen, e.g. bepaalde departementen, bedrijven, of enkel gemeenten, etc. (zie ‘organisatietypering’)



DIGITAAL VLAANDEREN

Vlaamse overheid

Voor wie? Doelgroepen

- De doelgroep bepaalt de beschikbare organisatiecode (hoewel in sommige gevallen ook een andere organisatiesleutel kan worden gevraagd)
- Uniek nummer van de organisaties per doelgroep:
  - Entiteiten van de Vlaamse Overheid (departementen, agentschappen): “GID”
    - OVO-code
  - Lokale Besturen (provincies, steden, gemeenten, politiezones, etc.) “LB”
    - KBO-code (evt. NIS-code, OVO-code)
  - Onderwijs- en Vormingsinstellingen (scholen, universiteiten, CLB’s, etc.): “OV”
    - Instellingsnummer
  - Bedrijven en andere organisaties (organisaties met een KBO-nummer): “EA”
    - KBO-nummer
- Zie voor een overzicht van organisatiecodes de KBO of Wegwijs

Inschatting aantal gebruikers

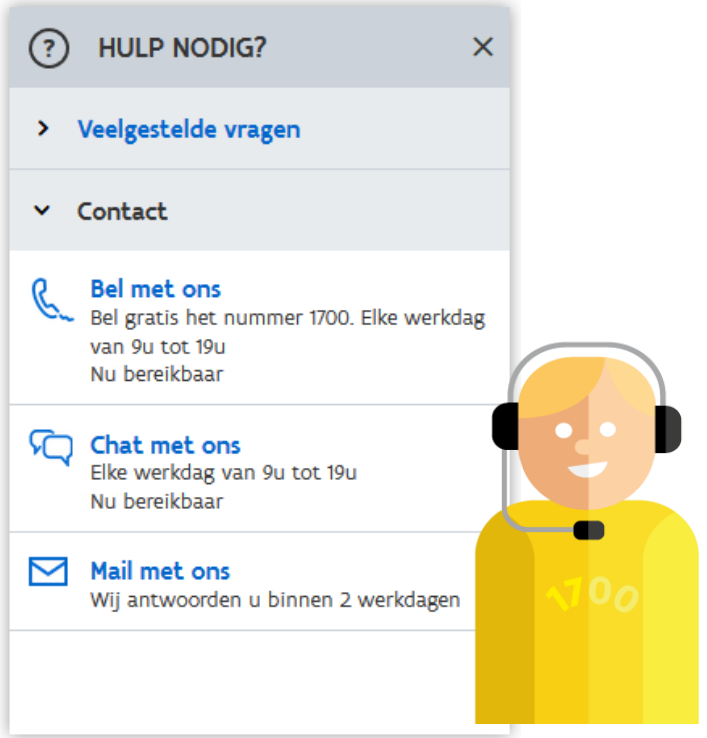
- Een idee van het verwachte aantal gebruikers en authenticaties helpt ons om de juiste capaciteit en ondersteuning te bieden
  - Inschatting verwachte aantal gebruikers
  - Inschatting verwachte aantal authenticaties
  - Betreft het een kantoorurentoepassing?
  - Zijn er piekperiodes? (e.g. de 'tax-on-web' periode)

- Zijn er ook gebruikers uit het buitenland?
  - Ook buitenlanders dienen te beschikken over een manier om zich aan te melden
  - Zie hiervoor onze presentatie over de BIS-Desk en eIDAS

Centrale ondersteuning i.s.m. ‘1700’

- Voor de eindgebruikers wordt de centrale helpdesk aangeboden waar ze terecht kunnen via telefoon, chat en mail (van 9u – 19u)
  - Eerstelijn = gratis door 1700 (e.g. “Hoe activeer ik Itsme?”)
  - Tweedelijns = gratis door HFB (e.g. “Ik kan mij authenticeren, maar ACM zegt dat ik niet de juiste rechten heb?”)
  - **Derdelijn = toepassing en helpdesk van klant (vaak inhoudelijke vragen).**

- Wie kan onze helpdesk contacteren voor derdelijnssupport?
  - Liefst een functionele mailbox



DIGITAAL VLAANDEREN | Vlaamse overheid

URL’s toepassing

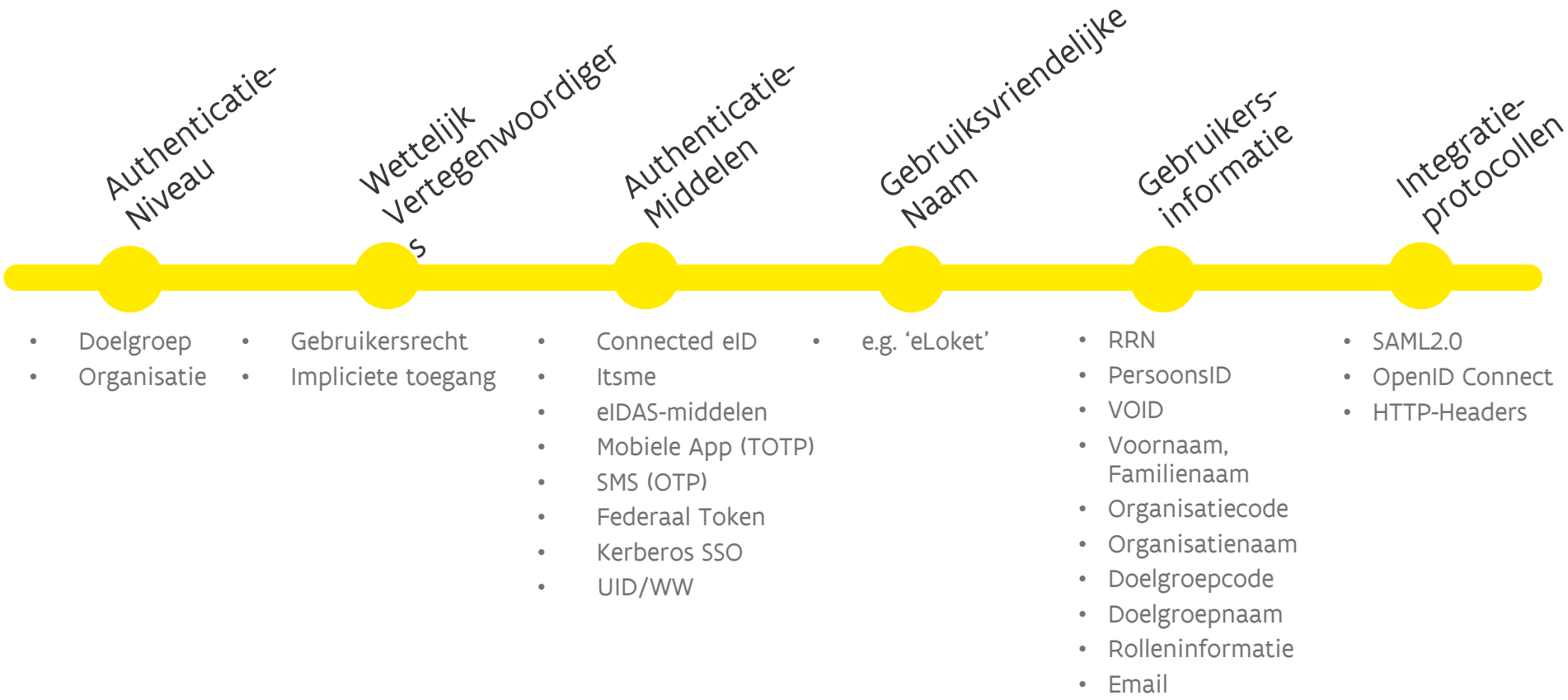
- Wat zijn de URL’s van de toepassing?
  - Waar een gebruiker zijn authenticatie zou starten
  - Bijvoorbeeld www.gemeenteloket.be, of departement.be/subsidies
- Zowel testomgevingen als productieomgevingen
  - Er kunnen verschillende testomgevingen van de klant aan de testomgeving (T&I) van ACM/IDM gekoppeld worden
- Welke doelgroepen hebben toegang tot welke URL?
  - Bijvoorbeeld, een toepassing staat open voor Burgers, Bedrijven (EA), en Het Facilitair Bedrijf (GID)
    - URL www.eloket.be/subsidies is bedoeld voor burgers en bedrijven
    - URL www.eloket.be/backofficeportaal is bedoeld voor medewerkers van HFB

2. Toegangsbeheer (ACM)

DIGITAAL VLAANDEREN

Vlaamse overheid

Belangrijkste onderwerpen ACM



DIGITAAL VLAANDEREN

Vlaamse overheid

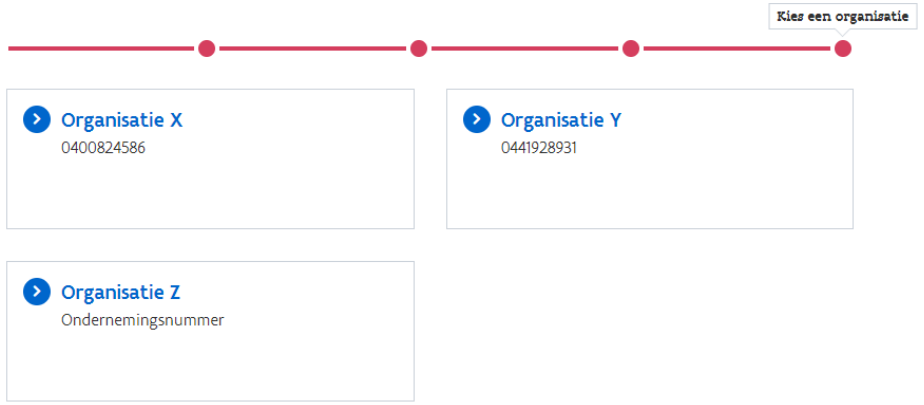
Authenticeren op doelgroep of organisatie

- Toepassingen kunnen de eindgebruiker op twee niveaus zijn hoedanigheid laten kiezen (‘als medewerker van’, geldt niet voor burgers): op doelgroepniveau of organisatieniveau

  - Doelgroepniveau
    - Gebruiker selecteert de doelgroep (hoedanigheid) waarvoor hij/zij wenst in te loggen
    - Indien de gebruiker het gebruikersrecht in kwestie heeft op meerdere organisaties zal de rolleninformatie alle organisatiecodes (KBO Nummer) bevatten
    - Voordeel: de toepassing krijgt alle rolleninformatie door en kan documenten voor meerdere organisaties naast elkaar weergeven

  - Organisatieniveau
    - Gebruiker kiest eerst de doelgroep zoals hierboven en kiest vervolgens de organisatie binnen die doelgroep waarvoor hij wenst in te loggen
    - ACM verwijst de gebruiker naar de toepassing met de rolleninformatie van de eindgebruiker voor deze organisatie
    - Voordeel: de toepassing krijgt enkel rolleninformatie voor één organisatie en moet zelf geen functionaliteit voor organisatiekeuze voorzien om documenten van meerdere organisaties van elkaar te scheiden

Authenticeren op doelgroep of organisatie



- Doelgroepkeuze
  - Identityticket bevat 1 of meerdere organisaties waar gebruiker het nodige recht voor heeft, e.g.
  - “LoketGebruiker:OrgX, OrgY, OrgZ”
  - Doelgroep bepaalt de organisatiecode, e.g. KBO-nr

- Organisatiekeuze
  - Identityticket bevat enkel de autorisatieinformatie van de gekozen organisatie, e.g.
  - “LoketGebruiker: OrgY”
  - Doelgroep bepaalt de organisatiecode, e.g. KBO-nr

DIGITAAL VLAANDEREN Vlaamse overheid

Authenticeren op doelgroep of organisatie

- Bijkomende opmerkingen
  - De keuze wordt automatisch voor de gebruiker gemaakt indien
    - De toepassing maar open staat voor 1 doelgroep
    - De gebruiker maar (de toepassingsspecifieke) rechten heeft namens 1 organisatie

- Authenticeren op organisatieniveau is om technische redenen niet mogelijk voor de doelgroep Onderwijs- en Vormingsinstellingen (OV)

Aanmelden voor wettelijk vertegenwoordigers

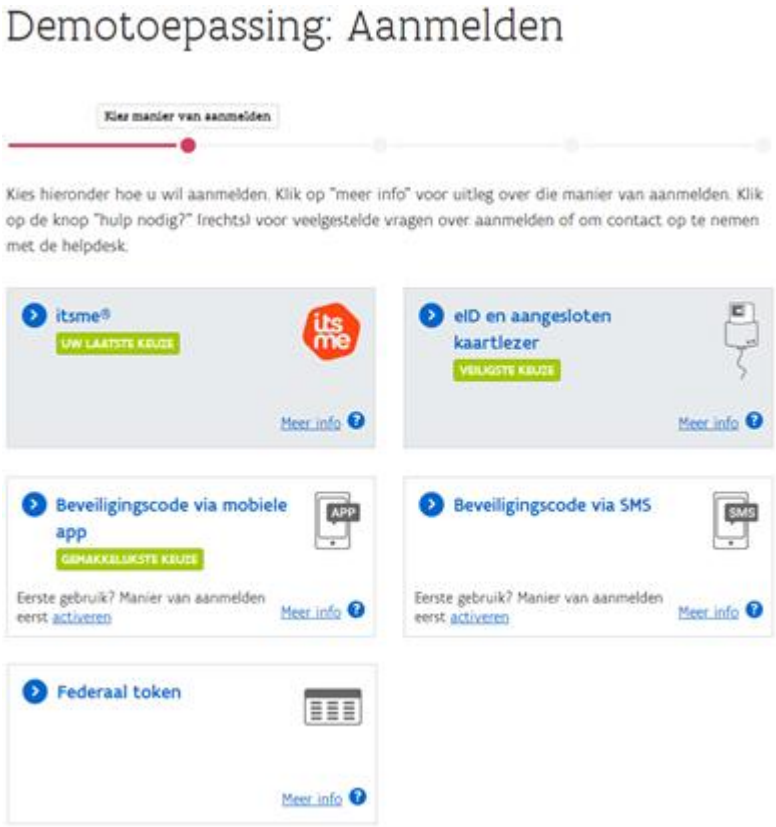
- ACM kan gebruikers ook authenticeren op basis van hun hoedanigheid als ‘wettelijk vertegenwoordiger’ van een onderneming
  - De gebruiker dient hiervoor ingeschreven te staan in het KBO als wettelijk vertegenwoordiger (i.e. zaakvoerder/bestuurder/etc)van die onderneming

- Deze optie is met name een voordeel voor kleine ondernemers.
  - Aanmelden voor ondernemers is niet altijd even eenvoudig; voor kleine ondernemers is deze functionaliteit daarmee een uitkomst

- Het nadeel van deze optie is dat de gebruiker wordt ingelogd als wettelijk vertegenwoordiger, en dus geen rechteninformatie wordt meegestuurd
  - De toepassing dient zelf een mapping te maken van de hoedanigheid op de rechten in de toepassing o.b.v. het uitgeleverde ticket (“WettelijkVertegenwoordiger:OrgX”)

Authenticatiemiddelen

- De getoonde authenticatiemiddelen in het ACM-scherm kunnen worden geconfigureerd per toepassing:
  - Connected eID
  - Eidas high
  - Itsme
  - eIDAS-middelen
  - Mobiele App (TOTP)
  - Eidas substantial
  - SMS (OTP)
  - Federaal Token
  - CBA (Certificate Based Authenticatie)
  - Kerberos SSO (enkel VO, ALFA AD)
  - UID/WW (niet sterk!)
- Mogelijke middelen zijn in functie van het vereiste veiligheidsniveau in overleg met uw veiligheidsconsulent

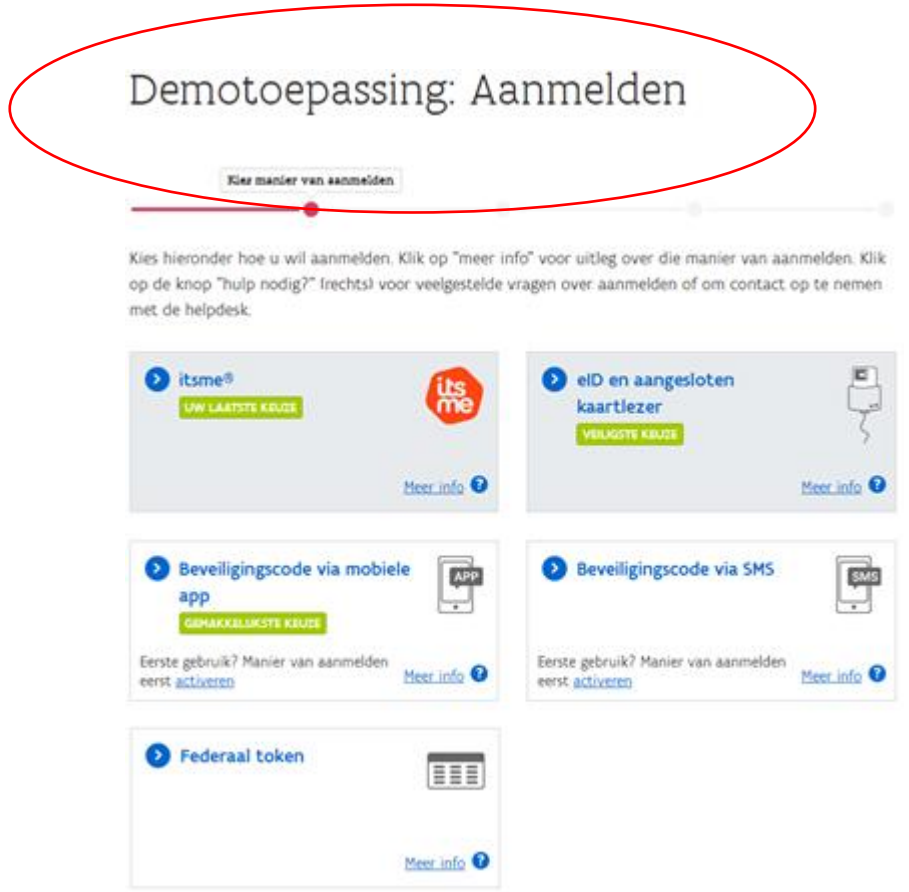


DIGITAAL VLAANDEREN

Vlaamse overheid

Gebruiksvriendelijke naam

- De naam van de toepassing kan worden geconfigureerd in het aanmeldscherm van ACM
  - E.g. ‘Overheidsloket’, altijd gevolgd door ‘Aanmelden’.
- De naam kan worden gekozen per aangesloten URL



Authenticatie-Niveau

Authenticatie-Middelen

Gebruiksvriendelijke Naam

Gebruikersinformatie (attributen)

Sommige attributen (stukjes gebruikersinformatie) zijn enkel beschikbaar in het geval de burger in de hoedanigheid van een organisatie inlogt.

- E.g. voor burgers is er vanzelfsprekend geen organisatiecode beschikbaar
- Uitgeleverde attributen kunnen ook gekozen worden per doelgroep

Denk goed na over welke informatie echt nodig is van welke gebruikers

- Dataminimalisatie = enkel meesturen waar nood/doel is (finaliteit)
- Verwerking van het Rijkregisternummer is gebonden aan wettelijke voorwaarden, maar op verantwoordelijkheid van de afnemer

Eventueel kan informatie ook uit externe bronnen worden opgehaald, afhankelijk van de nood van de toepassing (e.g. eHealth)

Gebruikersinformatie (attributen)

Naast enkel de autorisatie kan ACM ook gebruikersinformatie meesturen. De meest courante attributen zijn (meer in overleg mogelijk)

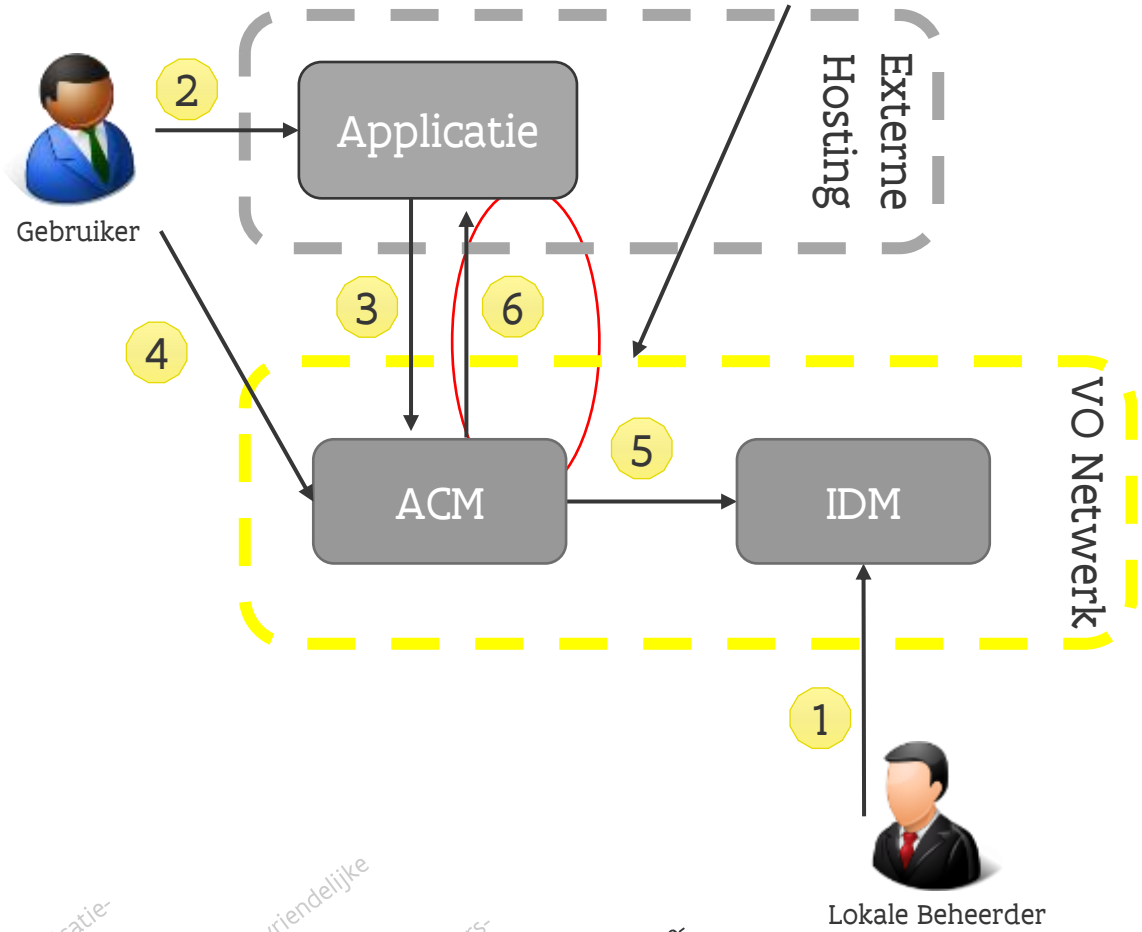
- Rijksregisternummer (Indien toegestaan)
- PersoonsID (gehashte vorm van Rijksregisternummer)
- VOID (unieke UID uit Gebruikersbeheer)
- Voornaam, Familienaam
- Organisatiecode (afhankelijk van doelgroep e.g. KBO-nummer, OVO-code)
- Organisatienaam (volledige organisatienaam)
- Doelgroepcode (GID, EA, LB, OV)
- Doelgroepnaam (Uitgeschreven doelgroepnaam, e.g. Economische Actoren)
- Rolleninformatie (e.g. “Gebruikersrecht-Context:Organisatiecode”, zie verder)
- Email (indien beschikbaar, vanuit IDM of CSAM Mijn Digitale Sleutels)

ACM-integratie realiseren

Hoe de koppeling maken tussen ACM en je toepassing?

1. De Lokale Beheerder geeft medewerkers gebruikersrechten in IDM;
2. De eindgebruiker surft naar de applicatie;
3. De applicatie stuurt de gebruiker naar ACM;
4. De gebruiker meldt aan en ACM authentiseert de eindgebruiker
5. ACM leest (indien van toepassing) rolleninformatie uit het Gebruikersbeheer,
6. ACM stuurt de autorisatiebeslissing en gebruikersinformatie terug naar de applicatie

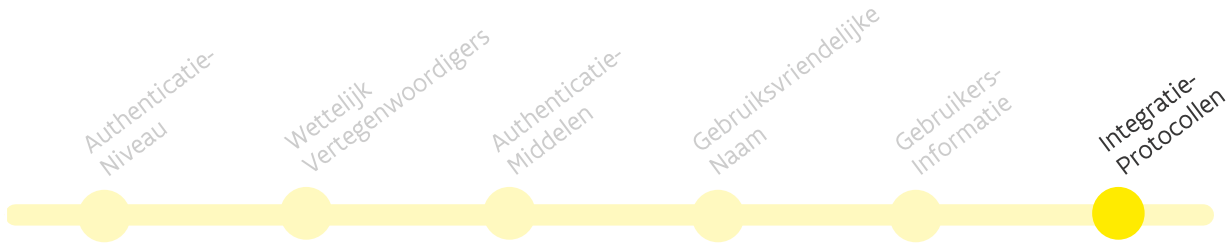
De gebruiker is nu ingelogd!



Beschikbare integratieprotocollen

- Voor de technische koppeling met ACM kan gebruik worden gemaakt van de open standaarden:
  - Federatie
    - OpenID Connect (authorisation code flow)
    - SAML2.0
  - Reverse Proxy
    - HTTP-Headers

- Voor meer (technische) informatie over de integratieprotocollen, zie onze aparte presentatie op de website.

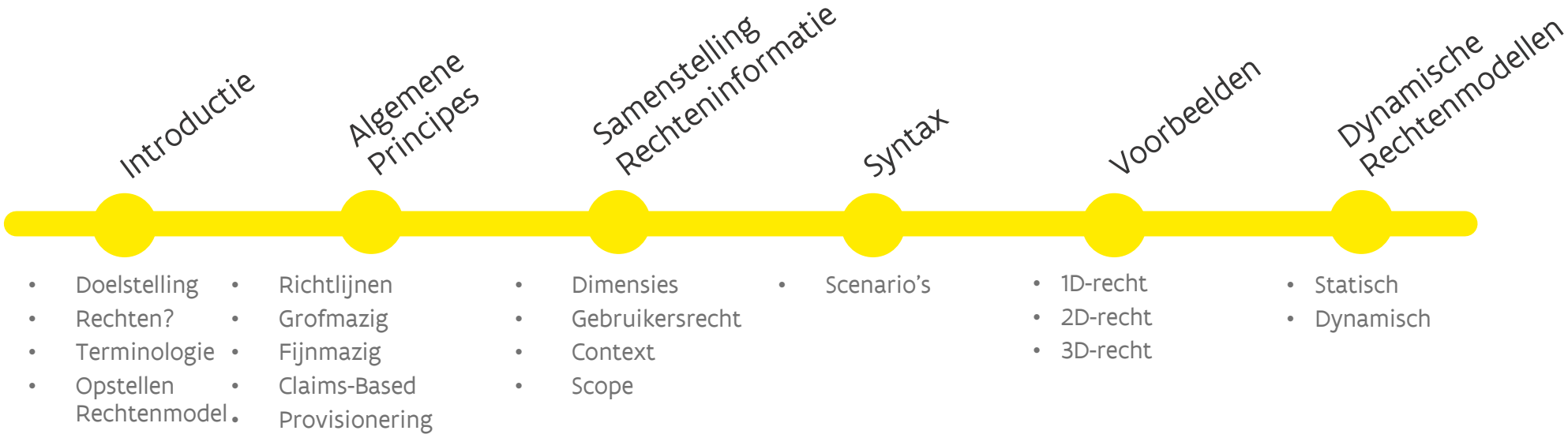


3. Gebruikersbeheer (IDM)

DIGITAAL VLAANDEREN

Vlaamse overheid

Belangrijkste onderwerpen IDM



DIGITAAL VLAANDEREN Vlaamse overheid

Doelstelling

- Deze slides zijn bedoeld om de klant te helpen bij het opstellen van een effectief model voor toegang van de eindgebruikers: het “rechtenmodel”
- Het integratieteam adviseert en begeleidt je graag in het opstellen van het rechtenmodel; deze slides zijn vooral bedoeld als hulpmiddel om zelf ook aan de slag te kunnen
- Het integratieteam configureert het rechtenmodel in het Gebruikersbeheer (testomgeving en productieomgeving), de klant test deze end-to-end
- Ook toekomstige wijzigingen verlopen via configuratie door het integratieteam

Wat zijn rechten?

- Toepassingen delegeren authenticatie en autorisatie naar het Toegangsbeheer
  - Authenticatie: Is de gebruiker wie hij beweert te zijn? (Of: wie is?)
  - Autorisatie: Mag deze gebruiker wel in de toepassing? (Of: wat mag?)
    - Namens de geselecteerde partij – op persoonlijke titel of namens een organisatie.

- Op autorisatieniveau kunnen twee niveaus van toegang worden onderscheiden:
  - Grofmazige toegang: De Gebruiker mag (of mag niet) in de toepassing.
  - Fijnmazige toegang: Als wat mag de gebruiker (namens deze partij) in de toepassing?
    - Denk aan “Lezer”, “Beheerder”, “Indiener”, “Auditor”, “Aanvrager”, etc.

- Het Toegangsbeheer voorziet de toepassing, indien gewenst, van de rechteninformatie.
  - De rechteninformatie wordt meegeleverd als attribuut in het identity token.
  - Het Toegangsbeheer haalt deze informatie op uit het Vlaams Gebruikersbeheer.

Woordenschat rond rechten

- Verschillende toepassingen en oplossingen gebruiken verschillende termen voor rechten:
  - Rol, recht, profiel, groep, entitlement, privilege, context, …

- Rechten in het Vlaams Gebruikersbeheer
  - Rechten: In het Gebruikersbeheer spreken we van rechten en rechtentoekenningen.
  - Contexten: De keuzes binnen een recht, indien van toepassing, noemen doorgaans ‘contexten’. Die kunnen slaan op rollen, profielen, etc. binnen de doeltoepassing.
    - Binnen in de rechten hanteren we de gangbare termen voor die toepassing.
    - Vaak komen rollen, profielen, groepen, etc. voor als actoren in de procesmodellen van de toepassing.

Opstellen van een rechtenmodel

- Gedelegeerd gebruikersbeheer is het standaardmodel binnen het Gebruikersbeheer
  - Organisaties (eindgebruikers) kennen een of meerdere Lokale Beheerders; dit zijn verantwoordelijken voor beheer van gebruikers en rechten binnen hun eigen organisatie:
    - Maakt identiteiten aan
    - Legt werkrelaties tussen gebruikers en zijn organisatie
    - Kent rechten toe
- Toepassingseigenaren (beheer van de toepassing) zijn daarom verantwoordelijk voor:
  - het opstellen van het rechtenmodel (samen met integratieteam)
  - bepalen welke organisaties (potentieel) de rechten mogen toekennen aan hun medewerkers
  - nooit voor het uitdelen van de daadwerkelijke rechten aan gebruikers
  - Ook de platformeigenaar (Vlaams Gebruikersbeheer) deelt in principe geen rechten uit
- Het integratieteam helpt je graag bij het opstellen van een optimaal rechtenmodel.

Algemene richtlijnen voor rechtenmodellen

- Vanuit het Gebruikers- en Toegangsbeheer streven we volgende principes na voor rechtenmodellen:

- Het Toegangsbeheer levert rechten- en rolleninformatie uit aan de toepassing.
- Toepassingen moeten een eenvoudig en statisch rechtenmodel nastreven.
- Lokale Beheerders moeten het rechtenmodel gemakkelijk begrijpen én met minimale inspanningen kunnen toekennen en beheren.
  - Een beperkt en duidelijk rechtenmodel is gemakkelijk te begrijpen, bijvoorbeeld rollen als ‘indiener’ en ‘raadpleger’ of ‘medewerker’ en ‘verantwoordelijke’.
  - Ingewikkelde rechten en rollenmodellen leiden tot onduidelijkheid bij de eindgebruiker en verhoogde complexiteit in beheer
  - Een Lokale Beheerder heeft minder werk met het onderhoud van rechtentoekenningen in het Gebruikersbeheer (periodieke hercertificering) als er een beperkt aantal rollen is voor een toepassing.

Grofmazige- en fijnmazige toegang

- Het rechtenmodel wordt gebruikt door het Toegangsbeheer voor grofmazige toegangscontrole
  - Toegangsbeheer authenticeert de gebruiker en beslist of de rechteninformatie voldoet aan de vereisten om toegang te krijgen tot de toepassing.
  - Toegangsbeheer voorziet de toepassing van gebruikersinformatie en rechteninformatie
  - De toepassing past, indien nodig, fijnmazige autorisatiecontroles toe op basis van de gebruikers- en rechteninformatie die het Toegangsbeheer uitlevert.
  - De toepassing maakt een sessie aan voor de gebruiker

Claims based authenticatie

- Het Toegangsbeheer levert binnen een standaard integratie alle gebruikersinformatie aan de toepassing tijdens het aanmelden.
  - Hieruit volgt dat de toepassing geen lokaal gebruikersbestand met actuele autorisatie-informatie kan aanhouden (immers, autorisatie-informatie wordt bijgehouden in het Gebruikersbeheer, en indien daar iets wijzigt, e.g. een rol wordt weggenomen, weet de toepassing dit niet totdat een gebruiker weer probeert in te loggen).
  - De toepassing kan wel informatie over gebruikers opslaan die het Toegangsbeheer heeft uitgeleverd bij authenticatie (e.g. de naam).

Provisionering

- Binnen een standaard traject schrijft het Gebruikersbeheer geen gebruikers- of rechteninformatie weg naar de toepassing via web services of andere mechanismes.
  - Gebruikers dienen ‘on the fly’ via Just-in-Time (JIT) provisioning te worden aangemaakt.
  - Het is echter technisch wel mogelijk dat het Gebruikersbeheer informatie provisioneert naar doelsystemen, e.g. naar AD-groepen, via een SOAP of SCIM protocol.
  - Denk aan gevallen waarbij gebruikers gekend moeten zijn voor de eerste login.
  - Dit valt buiten de standaard (een kost en offerteproces zijn van toepassing!).
  - Contacteer hiervoor het integratieteam; de ervaring leert dat in veel gevallen JIT-provisionering volstaat.

Samenstelling van rechtenmodel

DIGITAAL VLAANDEREN

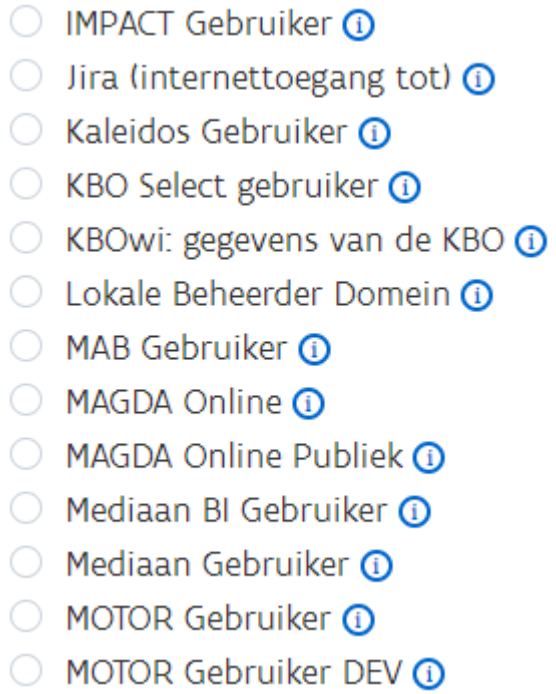
Vlaamse overheid

Dimensies in het rechtenmodel

- Het rechtenmodel van het Gebruikersbeheer kan in een standaard traject één, twee of drie parameters of dimensies gebruiken (1D, 2D of 3D). De standaardwaarden zijn:
  - **Gebruikersrecht**
    - Verwijst meestal naar grofmazige toegang.
    - Bezitten van gebruikersrecht “Toepassing Gebruiker’ geeft toegang tot de toepassing.
  - **Context**
    - Een verfijning van het Gebruikersrecht (fijnmaziger)
    - Voorbeelden zijn een ‘lezer’, ‘verantwoordelijke’, ‘beheerder’, ‘helpdeskmedewerker’, etc.
  - **Scope**
    - Een organisatiedimensie die de rechtentoekenning limiteert.
- Standaard wordt de rechteninformatie als volgt geconfigureerd (en uitgeleverd door het Toegangsbeheer)
  - “Gebruikersrecht-Context:Scope” (e.g. “SubsidiesGebruiker-Indiener:0329293939”)

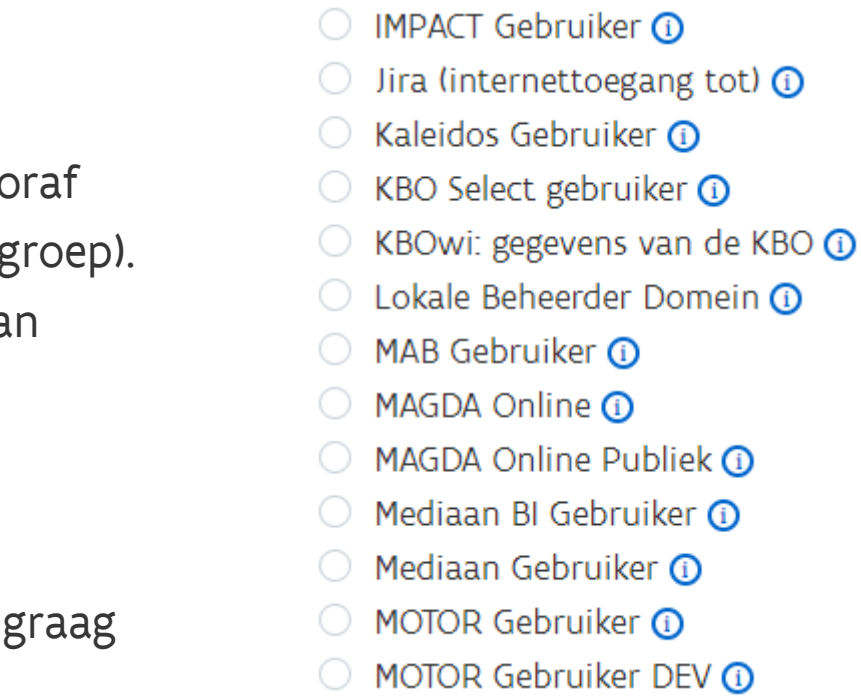
Gebruikersrecht

- Gebruikersrechten zijn de zichtbare en toekenbare rechten in het Gebruikersbeheer.
  - Dit zijn rechten die moeten worden verstaan door de Eindgebruiker en de Lokale Beheerder.
- Gebruikersrechten worden doorgaans gedefinieerd op niveau van de toepassing (weerspiegelt grofmazige toegang).
  - Bijvoorbeeld, voor de toepassing ‘Subsidiebeheer’ wordt een gebruikersrecht ‘Subsidiebeheer Gebruiker’ gedefinieerd.
  - Soms kan dit niet de beste oplossing zijn; het Integratieteam helpt u graag de afweging maken.
- Rechten zijn toekenbaar door Lokale Beheerders aan medewerkers van organisaties in een of meerdere doelgroepen:



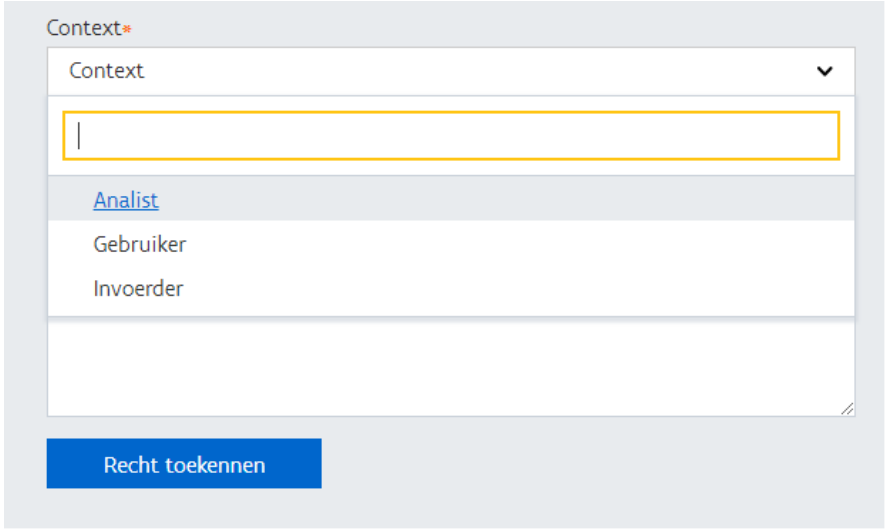
Gebruikersrecht (restricties)

- Standaard is een recht zichtbaar en toekenbaar aan alle organisaties binnen die doelgroep.
- Soms zijn rechten enkel zichtbaar en toekenbaar aan vooraf bepaalde groeperingen van organisaties (binnen de doelgroep). Het Gebruikersrecht kan dan enkel worden toegekend aan medewerkers van één van die organisaties (bijv., enkel 'Gemeenten' of 'Energieleveranciers').
  - Zie 'organisatietype restrictie' (andere presentatie).
- Tijdens het integratie proces helpt het integratieteam u graag de juiste keuze maken in functie van veiligheid en gebruikersgemak.



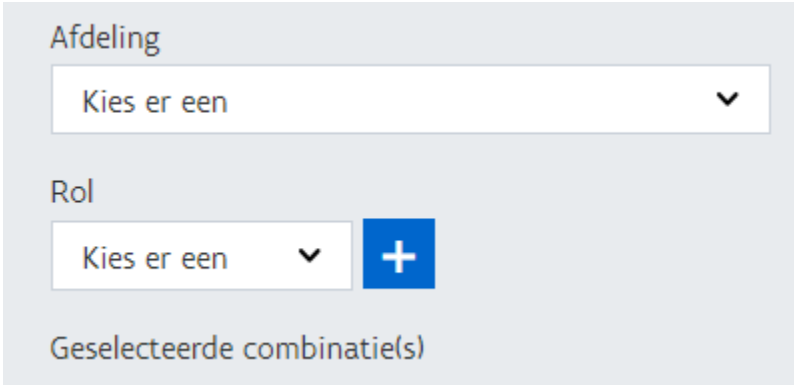
Context

- Contexten zijn een (optionele) verfijning van het Gebruikersrecht en bepalen doorgaans wat de Gebruiker mag binnen de toepassing.
  - Vaak de interne rechten van de toepassing, e.g. ‘lezer’, ‘indiener’, etc.
- De naam ‘context’ kan worden aangepast in de configuratie, naar bijvoorbeeld ‘Profiel’, ‘Privilege’, etc.
- Contexten kunnen worden gedefinieerd per Gebruikersrecht en per Doelgroep.
  - Bijvoorbeeld, voor de Gebruikersrecht ‘Subsidiebeheer Gebruiker’:
    - In de doelgroep VO medewerkers (GID) mag worden getoond: ‘Beheerder’ en ‘Back-office medewerker
    - In de doelgroep Bedrijven (EA) mag worden getoond: ‘Analist’, ‘Gebruiker’, en ‘Invoerder’.
- In de schermen zijn verschillende opties mogelijk om een context toe te kennen, bijvoorbeeld via een drop-down, of een meerkeuzelijst.



Context

- In sommige gevallen is een extra niveau van fijnmazigheid vereist. In dat geval kan worden gewerkt met ‘dubbele contexten’.
  - Bijvoorbeeld, in de toepassing “Subsidiebeheer” is een gebruiker ‘verantwoordelijke’, maar enkel voor onderdeel ‘subsidie-aanvragen’, terwijl hij slechts ‘controleur’ is voor het onderdeel ‘subsidiebetalingen’.
  - Denk ook aan portaalwebsites, waar 1 Gebruikersrecht wenselijk is voor toegang tot het portaal, maar achter het portaal meerdere toepassingen draaien met elk hun eigen rollen.
  - Andere use-cases kunnen fijnmaziger organisatiebeheer zijn.
- In de praktijk:
  - Compliceert een dubbele context het rollenmodel onnodig.
  - Dekt een enkele context vaak alle noden af.
  - Kan ook het Gebruikersrecht worden opgesplitst.
  - De keuze zal verschillen per toepassing; het integratieteam helpt u graag de juiste afweging maken.



Scope

- Rechtentoekenningen zijn gelimiteerd op een organisatie
  - Men krijgt een recht voor de toepassing maar enkel voor een bepaalde organisatie.
  - Naar een organisatie limitering verwijzen we binnen het gebruikersbeheer in technische documenten met "*scope*".
  - Praktisch kan een Gebruiker voor verschillende organisaties hetzelfde recht hebben, of juist verschillende rechten.
    - Bijvoorbeeld, Gebruiker is 'verantwoordelijke' voor organisatie A, maar slechts 'medewerker' voor Organisatie B.

- Om deze reden bestaan geen rechten voor de doelgroep Burgers (Particulieren) in het Gebruikersbeheer!
  - Deze gebruikers loggen immers altijd in 'namens zichzelf'
  - Zij kunnen zichzelf niet beperken in rechten

Scope

- Afhankelijk van de doelgroep worden standaard de volgende organisatiesleutels uitgeleverd:
  - Vlaamse Overheden (GID): OVO-code
    - e.g. OVO002303
  - Economische Actoren (EA): KBO-nummer (of vestigingsnummer)
    - e.g. 0248.015.142
  - Lokale besturen (LB): KBO-nummer (evt. NIS-code)
  - Onderwijs- en vormingsinstellingen (O&V): Instellingsnummer
    - e.g. 36939
- Andere sleutels kunnen worden besproken met het Integratieteam.
- Voor een overzicht van de verschillende sleutels en organisaties, zie wegwijs.vlaanderen.be.

Dimensies in het rechtenmodel

- Naast de standaardparameters kunnen ook andere parameters in de rechteninformatie worden geconfigureerd:
  - Alle bekende attributen over de identiteit kunnen worden meegeleverd in de rechteninformatie (denk bijvoorbeeld aan emailadres, indien bekend).
  - Doorgaans worden deze attributen ook in de identity token meegeleverd, waardoor het niet nodig is deze informatie in de rechteninformatie weg te schrijven.

Rechtenmodel syntax

- Het Gebruikersbeheer schrijft informatie weg in een string formaat
  - dat een datastructuur bevat,
  - dat het Toegangsbeheer gemakkelijk in zowel XML, json, of http headers formaat kan verpakken.

Syntax naam	Syntax formaat	Toelichting
1D recht	<recht1> <recht2>	De gebruikersrechten geven de Gebruiker toegang tot de toepassing(en).
2D recht	<recht1>:<scopeA>	De Gebruiker heeft gebruikersrecht 1 namens OrganisatieA.
2D recht (multiscope)	<recht1>:<scopeA>,<scopeB> <recht2>:<scopeA>,<scopeC>	De gebruiker heeft het recht 1 voor Organisaties A en B, en recht 2 voor organisaties A en C.
3D recht (singlecontext, multiscope)	<recht1>-<contextX>:<scopeA>,<scopeB> <recht1>-<contextY>:<scopeA>,<scopeC>	De Gebruiker heeft hetzelfde recht, maar met verschillende contexten voor verschillende organisaties (gesorteerd op context): namelijk context X voor organisaties A en B, en context Y voor organisaties A en C.
3D recht (multicontext, singlescope)	<recht1>-<contextX>,<contextY>:<scopeA> <recht1>-<contextX>,<contextZ>:<scopeB>	De Gebruiker heeft hetzelfde recht, maar met verschillende contexten voor verschillende organisaties (gesorteerd op scope): Namelijk context X en Y voor Organisatie A, maar context X en Z voor organisatie B.

Voorbeelden

DIGITAAL VLAANDEREN

Vlaamse overheid

Fictieve toepassing “DossierPunt” als voorbeeld

- Toepassing DossierPunt van “het Agentschap” behandelt dossiers van verschillende categorieën voor ondernemingen.

- Actoren in DossierPunt:
  - Binnen het agentschap is er
    - Een ApplicatieBeheerder die technische parameters in de toepassing kan beheren
    - Een DossierBeheerder die alle dossiers in de toepassing kan beheren.
  - Binnen ondernemingen is er
    - Een OrganisatieVerantwoordelijke die dossiers van eender welke categorie opstart en finaal indient.
    - Een OrganisatieRaadpleger die dossiers van eender welke categorie kan raadplegen, maar niet opstarten, aanvullen of indienen.
    - Een OrganisatieMedewerker die dossiers van een specifieke categorie aanvult, maar niet opstart of indient.

Rechtenmodel voorbeelden: 1D recht

- Gebruiker is simpelweg ApplicatieBeheerder en DossierBeheerder
  - Dossiercategorie is niet van toepassing op deze rechten.
    - Er is dus geen contextkeuze “Dossiercategorie”.
  - Rechtentoekenningen zijn in dit geval niet organisatiespecifiek.
    - Er is dus geen scope relevant.
  - Gevolg: alle gebruikers met Applicatiebeheerder en Dossierbeheerder zien en kunnen exact hetzelfde in de toepassing Dossierpunt, er wordt geen onderscheid gemaakt.
- Uitgeleverde attribuutwaarden:
  - Federation:
    - ApplicatieBeheerder
    - DossierBeheerder
  - Reverse proxy:
    - ApplicatieBeheerder|DossierBeheerder

Rechtenmodel voorbeelden: 2D recht, multiscope

- Gebruiker is OrganisatieVerantwoordelijke voor org1 en org2, maar OrganisatieRaadpleger voor org2 en org3.
  - Beide rechten zijn gelimiteerd op de onderneming, maar niet op dossiercategorie. Er is dus wel een scope parameter, maar geen contextkeuze “Dossiercategorie”.

- Uitgeleverde attribuutwaarden:
  - Federation:
    - OrganisatieVerantwoordelijke:org1,org2
    - OrganisatieRaadpleger:org2,org3
  - Reverse Proxy:
    - OrganisatieBehandelaar:org1,org2|OrganisatieRaadpleger:org2,org3

Rechtenmodel voorbeelden: 3D recht, single context, multiscope

- Gebruiker is OrganisatieMedewerker voor CategorieA (A) en CategorieB (B) voor org1 en org2, maar voor CategorieA en CategorieC (C) voor org2 en org3

- Uitgeleverde attribuutwaarden:
  - Federation:
    - OrganisatieMedewerker-A:org1,org2,org3
    - OrganisatieMedewerker-B:org1,org2
    - OrganisatieMedewerker-C:org2,org3
  - Reverse Proxy:
    - OrganisatieMedewerker-A:org1,org2|OrganisatieMedewerker-B:org1,org2|OrganisatieMedewerker-C:org2,org3

Rechtenmodel voorbeelden: 3D recht, multi context, singlescope

- Zelfde toestand, anders weggeschreven: Gebruiker is OrganisatieMedewerker voor CategorieA (A) en CategorieB (B) voor org1 en org2, maar voor CategorieA en CategorieC (C) voor org2 en org3

- Uitgeleverde attribuutwaarden:
  - Federation:
    - OrganisatieMedewerker-A,B:org1
    - OrganisatieMedewerker-A,B,C:org2
    - OrganisatieMedewerker-A,C:org3
  - Reverse Proxy:
    - OrganisatieMedewerker-A,B:org1|OrganisatieMedewerker-A,B,C:org2|OrganisatieMedewerker-A,C:org3

Dynamische rechtenmodellen

DIGITAAL VLAANDEREN

Vlaamse overheid

Statische vs dynamische rechtenmodellen

- Een statisch rechtenmodel gebruikt enkel vooraf gedefinieerde parameters
  - Bijvoorbeeld een vaste lijst van vooraf gedefinieerde rollen, gelimiteerd op een vaste lijst van document types.

- Een dynamisch rechtenmodel gebruikt parameters die variëren op basis van transacties in business processen rond de toepassing.

  - Bijvoorbeeld rollen gelimiteerd op dossiernummers:
    - Het Gebruikersbeheer kan tijdens het toekennen van rollen door de Lokale Beheerder dossiernummers voor de organisatie van de Lokale Beheerder ophalen.
    - In de toepassing maakt een verantwoordelijke een dossier aan. De Lokale Beheerder kan in het Gebruikersbeheer onmiddellijk rollen toekennen gelimiteerd op dit pas aangemaakte dossier.

Standaard statisch rechtenmodel

- Waar mogelijk moeten toepassingen proberen om een statisch rechtenmodel te hanteren.
  - Een statisch rechtenmodel is eenvoudiger te begrijpen voor de Lokale Beheerder en operationeel goedkoper in ondersteuning.
  - Enkel waar een dynamisch rechtenmodel een duidelijke meerwaarde biedt zal het Gebruikersbeheer een dynamisch rechtenmodel overwegen.

- Een dynamisch rechtenmodel kan niet in een standaard traject.
  - Dit vanwege het opzetten van datastromen en de bijkomende ondersteuning die de toepassingen tijdens hun integratietraject nodig hebben; de rechten worden opgehaald door middel van een webservice.
  - Voor de integratie van de webservice langs de zijde van het Vlaams Gebruikers- en Toegangsbeheer worden kosten aangerekend.

4. Uitrol

DIGITAAL VLAANDEREN

Vlaamse overheid

Ondersteuning bij uitrol

- Wij kunnen u ook ondersteunen bij de uitrol van de toepassing naar de eindgebruikers, door voorlichtingsmaterialen of presentaties
  - Als klant heb je hierin wel altijd het voortouw, omdat je de eigen achterban zelf het beste kent
- Denk aan:
  - Folder digitale sleutels
  - Folder voor ondernemers
  - Handleiding
  - Tutorials
  - Helpdeskondersteuning van eindgebruikers
- Wij blijven graag op de hoogte van communicaties naar eindgebruikers, zodat we ook rekening kunnen houden met toestroom van gebruikers, bepaalde vragen voor onze helpdesk, etc.

Uploads in bulk naar het Gebruikersbeheer

- Het Gebruikersbeheer laat toe om grote acties die uitgevoerd dienen te worden, zoals rechten aan veel gebruikers toekennen, aan te leveren via gestructureerde en voorbepaalde informatie in tekstbestanden (.csv's).

- Bij de inproductiestelling van een integratie kan het ACM/IDM team ***eenmalig*** gebruikers in bulk opladen.
  - Hiervoor is menselijke tussenkomst nodig, vandaar enkel eenmalig
  - Dit kan enkel wanneer de lokale beheerder van de organisaties op een sluitende manier zijn goedkeuring voor de eindgebruikers van zijn organisatie kan geven.
- Geautomatiseerde uploads van gebruikersinformatie naar het gebruikersbeheer kunnen (nog) niet binnen een standaard traject en worden afgeraden

5. Partners

DIGITAAL VLAANDEREN

Vlaamse overheid

Mijn Burgerprofiel

- Integreren met Mijn Burgerprofiel vereist ook een integratie met het Toegangsbeheer, in 'light'-versie of een standaardintegratie voor volledige functionaliteit
- Toegangsbeheer levert naast de standaardintegratie aan de klant ook een 'AppID' uit die gebruikt wordt in de embedcode van Mijn Burgerprofiel
- Hiervoor is de origin-URL nodig van de klant : een URL dat enkel het domein en het protocol bevat (geen pad), bv.: https://test.vlaanderen.be

- Neem contact op met het integratieteam voor het gehele proces

- Zie ook: https://overheid.vlaanderen.be/mijn-burgerprofiel

Ondernemersloket

- Integreren met het Vlaams Ondernemersloket vereist ook een integratie met het Toegangsbeheer
  - Tijdens het integratieproces dient te worden aangegeven welke URL's ook zullen integreren met het Ondernemersloket (voorziet juiste functionaliteit bij wisselen van organisaties in het ondernemersloket)
  - Tijdens het configureren van de rechten dient te worden aangeven welke rechten bij de URL's horen die mee integreren bij het Ondernemersloket, en dus ook toegang moeten geven tot het Ondernemersloket, naast de eigen toepassing
  - Voor de rechten zal ook de zelfregistratiefunctionaliteit worden voorzien, zodat gebruikers in het Ondernemersloket rechten kunnen aanvragen
- Zie ook: https://www.vlaanderenonderneemt.be/

Contactinfo
Toegangs- en Gebruikersbeheer

- Online:
  - http://overheid.vlaanderen.be/gebruikersbeheer
  - http://overheid.vlaanderen.be/toegangsbeheer
- Toelichting over ons integratieproces
  - https://overheid.vlaanderen.be/acm/idm-standaard-aansluitingsproces
- Mailtje sturen?
  - Integraties.gebruikersbeheer@vlaanderen.be
- Ondersteuning via gratis nummer 1700
- Bekijk ook onze online filmpjes!!

DIGITAAL VLAANDEREN

Vlaamse overheid