Vlaams Gebruikers- en Toegangsbeheer

Kennismakingspresentatie

DIGITAAL VLAANDEREN

Vlaamse overheid

Wie zijn we en wat doen we?

DIGITAAL VLAANDEREN

Vlaamse overheid

Digitaal Vlaanderen

Digitaal Vlaanderen biedt professionele ondersteuning aan de entiteiten van de Vlaamse overheid in kennis en producten.

Digitaal Vlaanderen voorziet generieke, herbruikbare ICT-bouwstenen voor de Vlaamse overheid:

- Toegangsbeheer (ACM)
- Gebruikersbeheer (IDM)
- Certificatenbeheer (DCB)
- Digitaal ondertekenen (DTP en digitale handtekenmap)
- Digitale formulieren
- Digitaal betalen

DIGITAAL VLAANDEREN

Vlaamse overheid

Uitdagingen bij digitalisering van de overheid

Steeds meer overheidsprocessen worden gedigitaliseerd

- Burgers kunnen gemakkelijk online zaken doen met de Vlaamse overheid, bijvoorbeeld voor het aanvragen van subsidies, vergunningen, of attesten.

De overheidsdienst moet zekerheid hebben over de identiteit van de burger

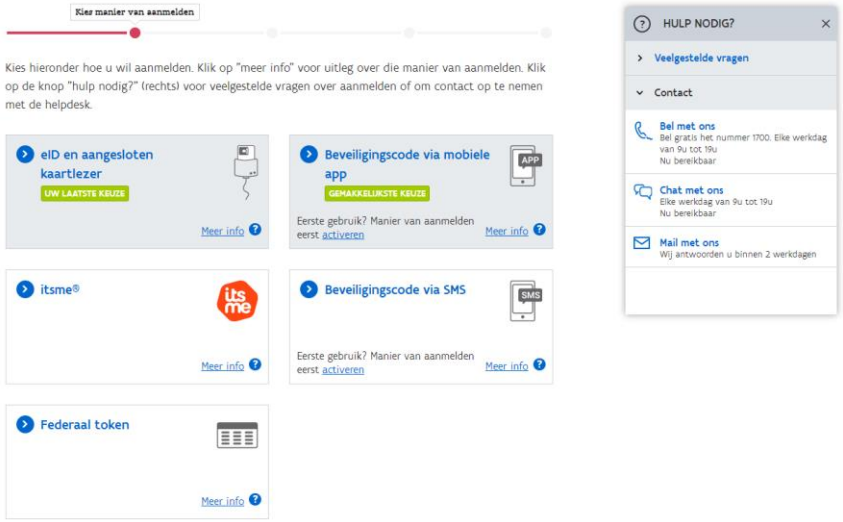
- Burgers komen niet meer naar een fysiek loket, en moeten online kunnen bewijzen wie ze zijn, voor wie ze werken, en wat ze mogen: een subsidie mag niet aan de verkeerde persoon of bedrijf worden uitgekeerd.

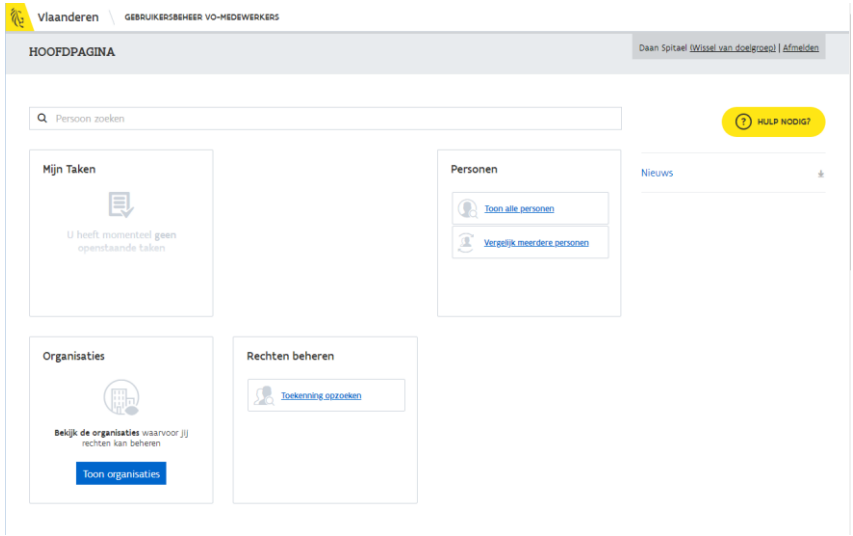
Ook de back-office processen worden gedigitaliseerd

- Toepassingen moeten tegenwoordig via het internet te bereiken zijn, maar alleen de eigen medewerkers mogen toegang hebben.

Hoe zorg ik voor gebruiksvriendelijk, veilig, schaalbaar, en voordelig beheer van toegang en gebruikers in mijn toepassing?

Twee bouwstenen





ACM: Toegangsbeheer

- Toegang krijgen
  - Aanmelden
  - Identificeren
  - Authenticeren

IDM: Gebruikersbeheer

- Toegang geven
  - Gebruikers en rechten beheren
  - Op één plaats
  - In real-time

DIGITAAL VLAANDEREN

Vlaamse overheid

Wat bieden we?

Het Vlaams Gebruikers- en Toegangsbeheer biedt een robuuste, veilige en bovenal gebruiksvriendelijke oplossing, conform privacywetgeving en marktstandaarden

We bieden meer dan enkel de bouwstenen: professionele begeleiding en deskundig advies op maat vormen de kern van onze dienstverlening

Ook na integreren van de bouwstenen bieden we operationele support voor eindgebruikers en toepassingsbeheerders

DIGITAAL VLAANDEREN Vlaamse overheid

Voor wie?

Het Vlaams Gebruikers- en Toegangsbeheer kan gebruikt worden zowel voor:

- **Interne** medewerkers ('back-office' van overheden, niet voor private bedrijven)
- **Externe** doelgroepen ('front-office'; burgers, medewerkers van organisaties)

Organisaties worden onderscheiden in de volgende doelgroepen:

- Entiteiten van de Vlaamse Overheid (departementen, agentschappen)
- Lokale Besturen (provincies, steden, gemeenten, politiezones, etc.)
- Onderwijs- en Vormingsinstellingen (scholen, universiteiten, CLB's, etc.)
- Bedrijven en andere organisaties (organisaties met een KBO-nummer)

Alle Vlaamse overheidsinstanties (entiteiten, lokale besturen, onderwijsinstellingen) kunnen de bouwstenen integreren in de eigen toepassingen (of softwareleveranciers namens deze overheden)

Voordelig businessmodel

Klanten integreren kosteloos binnen standaardtrajecten

- Digitaal Vlaanderen draagt de integratiekost voor zowel advies en expertise als voor de bouwstenen zelf
- Eigen kosten van integratie zijn voor de klant (eigen mensen, softwareontwikkeling)
- Geen operationele of volume gedreven kosten

Klanten profiteren van de schaalvoordelen van 1 centraal platform

- Operationele kosten en inspanning (bv. beschikbaarheid) worden centraal gedragen (één platform vs. elke applicatie afzonderlijk biedt duidelijke voordelen)
- Investering in verbeteringen en vernieuwingen komen ten goede aan alle gekoppelde toepassingen

We blijven verbeteren en vernieuwen in co-creatie met klant en eindgebruiker

- IT-technisch
- Gebruikersinterface
- Procesmatige en juridische evoluties
- Nieuwe componenten en functionaliteiten

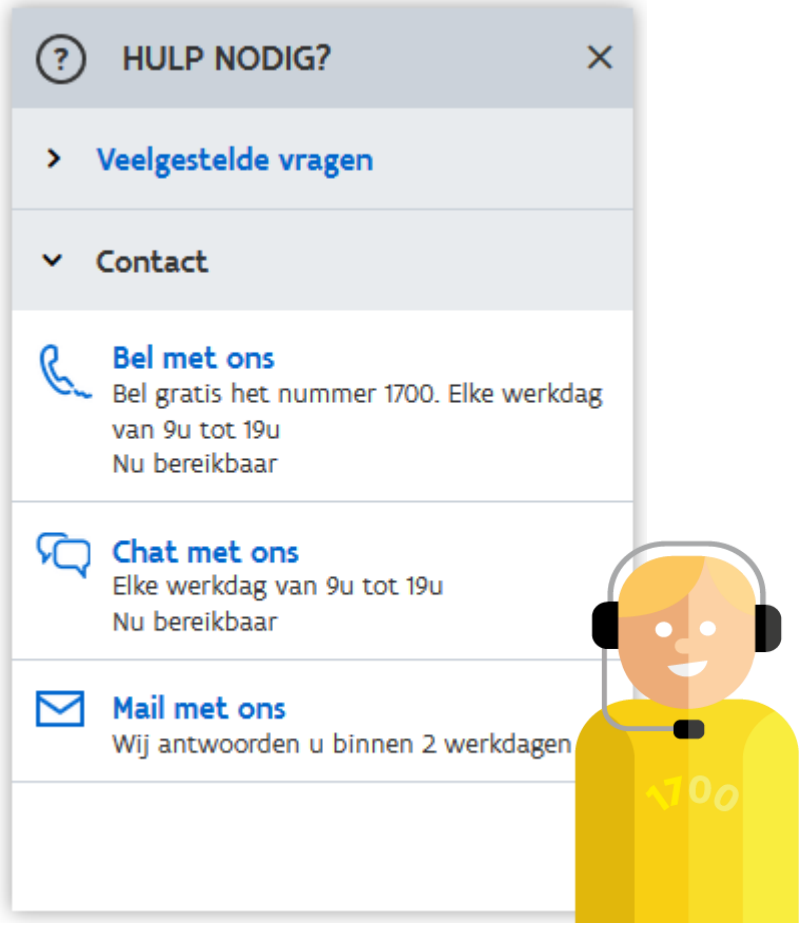
DIGITAAL VLAANDEREN

Vlaamse overheid

Centrale ondersteuning i.s.m. ‘1700’

Een centrale helpdesk waar eindgebruikers terecht kunnen via telefoon, chat en mail (van 9u – 19u)

- Eerste lijn = gratis door 1700 (e.g. “Hoe activeer ik Itsme?”)
- Tweede lijn = gratis door Digitaal Vlaanderen (e.g. “Ik kan mij authenticeren, maar ACM zegt dat ik niet de juiste rechten heb?”)
- Derde lijn = toepassing en helpdesk van klant (vaak inhoudelijke vragen).



DIGITAAL VLAANDEREN

Vlaamse overheid

Toegangsbeheer

DIGITAAL VLAANDEREN

Vlaamse overheid

Wat is het Toegangsbeheer?

Het Toegangsbeheer (ACM) draait om toegang krijgen door gebruikers te laten aanmelden

- ACM is de 'toegangspoort' naar toepassingen, en controleert of iemand naar binnen mag

ACM stelt gebruikers daarvoor in staat zich te identificeren en te authenticeren:

- Identificeren = claimen wie je bent ("Ik ben Piet")
- Authenticeren = kunnen bewijzen van de claim ("Dit is inderdaad Piet")

ACM laat gebruikers zich 'sterk authenticeren': bewijzen wie je bent met een hoog zekerheidsniveau over de identiteit van de gebruiker

- Door middel van authenticatiemiddelen, zoals een eID, Itsme, SMS-code, etc.
- Twee-factor authenticatie maakt de authenticatie sterk: de gebruiker moet 'iets weten' en 'iets hebben', zoals een eID-kaart en zijn pincode

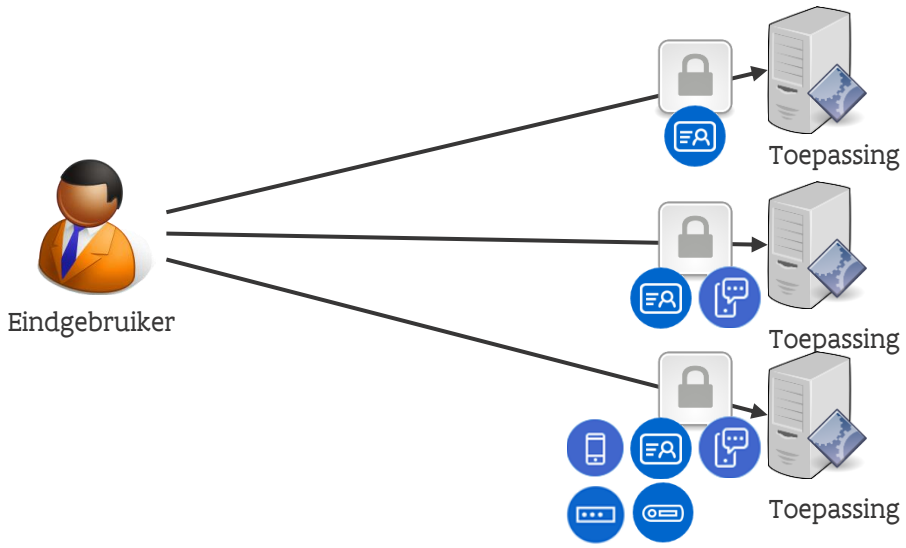
Use cases i.k.v. Toegangsbeheer

Gebruikers moeten zich voor veel toepassingen kunnen aanmelden.

Doorgaans betekent dit dat de gebruiker voor elke toepassing een apart aanmeldingsmiddel nodig heeft, zoals weer een nieuw gebruikersnaam en wachtwoord.

Aanmeldingen kunnen niet gedeeld worden tussen toepassingen; je moet telkens opnieuw aanmelden.

Toepassingseigenaars moeten telkens zelf de nodige (kostbare) componenten voorzien.



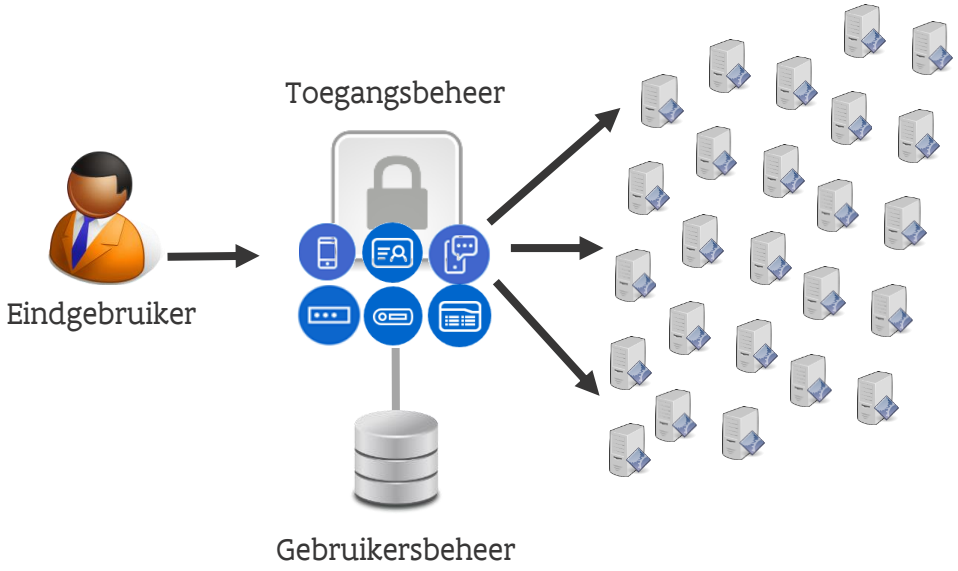
De oplossing via ACM - Toegangsbeheer

ACM maakt de digitale sleutels van de eindgebruiker herbruikbaar, ongeacht de toepassing waar hij/zij wil aanmelden.

De filosofie: het maakt niet uit met welke sleutel de eindgebruiker zich aanmeldt (mits voldoende veilig), zolang de gebruiker maar kan bewijzen wie hij/zij is.

Door de aanmelding via een centrale toegangspoort te regelen kan de gebruiker automatisch worden ingelogd op andere aangesloten toepassingen van de Vlaamse Overheid (**Single Sign On**).

Toepassingseigenaars kunnen gebruikmaken van een generieke, herbruikbare component.



Keuze van digitale sleutel / authenticatiemiddel

ACM laat de gebruiker kiezen met welk middel hij/zij het liefste ‘sterk’ aanmeldt, bijvoorbeeld met Itsme, of met een eID-kaart o.b.v. zijn/haar digitale sleutels.

- Het is aan de toepassingseigenaar om te kiezen welke sleutels de eindgebruiker mag gebruiken, i.f.v. het vereiste veiligheidsniveau
- Onderdeel van de configuratie

Sterk aanmelden is noodzakelijk voor ontsluiten van persoonsgegevens

Het herkenbare, uniforme aanmeldscherm van ACM wekt vertrouwen bij eindgebruikers

- Titel is aanpasbaar per toepassing

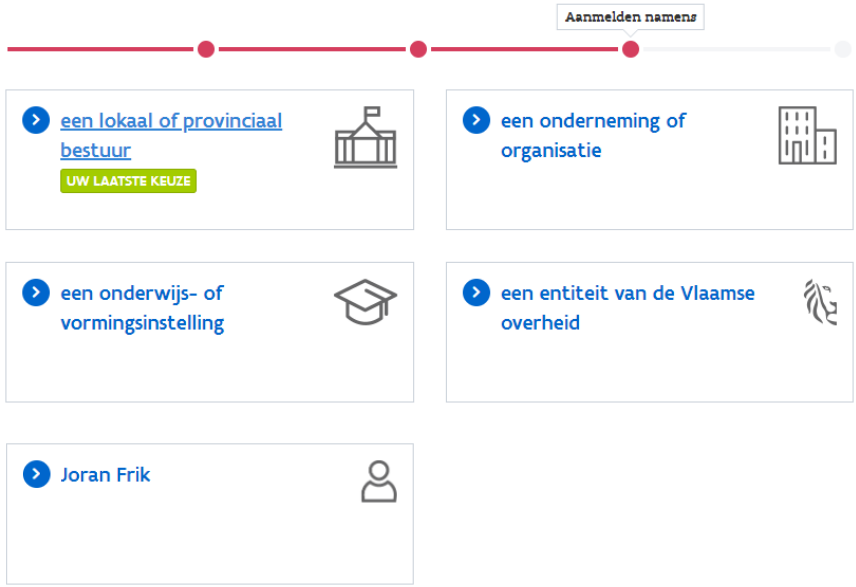
Inloggen namens een organisatie

ACM laat gebruikers toe in te loggen namens zichzelf of namens een organisatie

- Als ‘medewerker van een organisatie’

Zo biedt ACM de toepassing zekerheid over niet alleen de identiteit van de gebruiker, maar ook over de hoedanigheid waarin deze een actie wenst uit te voeren

- Gebruikers dienen een werkrelatie te hebben met de organisatie in het Gebruikersbeheer (zie verder)
- Afhankelijk of de organisatie binnen de gekozen doelgroep van de toepassing valt (configuratie)



DIGITAAL VLAANDEREN
Vlaamse overheid

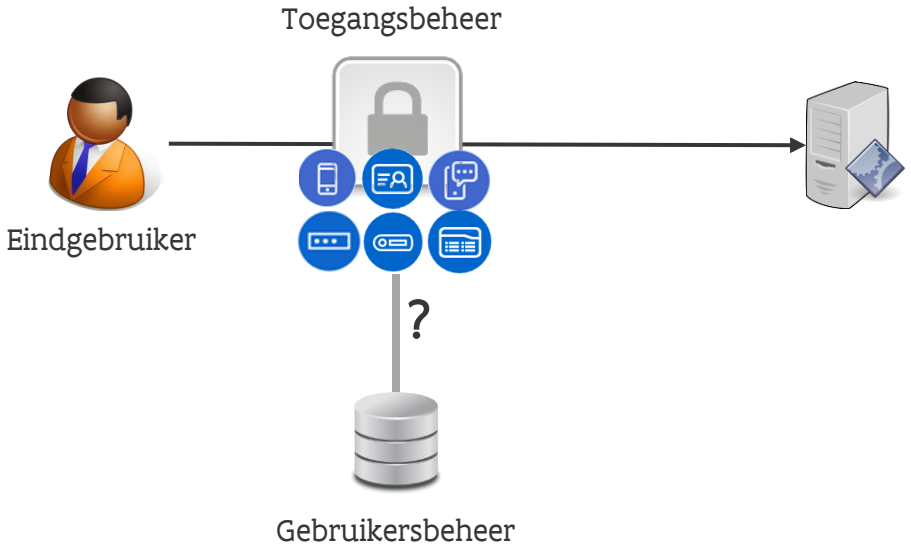
Wie mag binnen: autorisatiebeslissingen

ACM controleert of iemand binnen mag in de toepassing of niet (autorisatiebeslissing)

De beslissing wordt genomen op basis van externe bronnen, waarvan het Gebruikersbeheer de belangrijkste is

- Voor medewerkers namens een organisatie is een Gebruikersrecht nodig
- Burgers (particulieren namens zichzelf) hoeven zich enkel sterk te authenticeren.

De autorisatieregels (wie mag binnen en wie niet) zijn een belangrijk onderdeel van het integratie proces dat we samen doorlopen



Doorgeven gebruikersinformatie

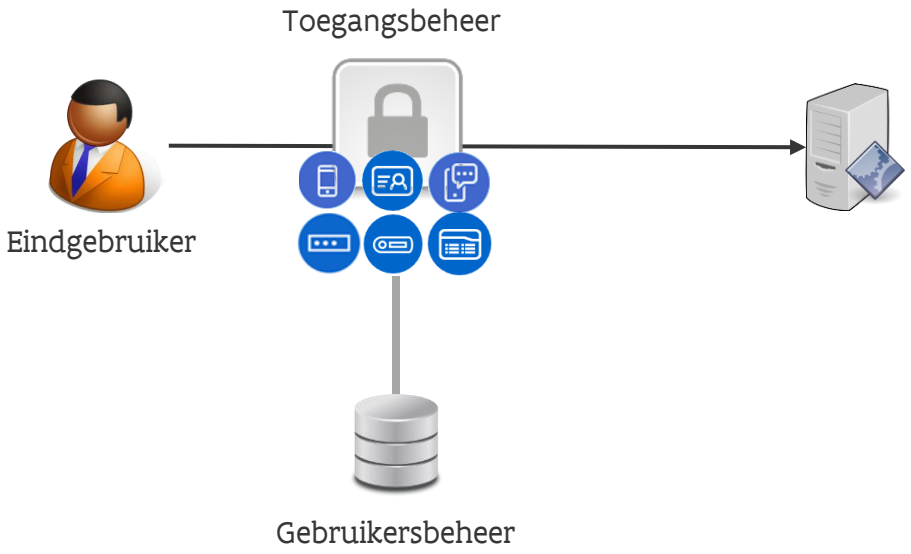
ACM maakt zelf grofmazige autorisatiebeslissingen (rol van toegangspoort)

ACM stuurt, indien gewenst, extra informatie mee voor fijnmazige beslissingen door de toepassing

Typische attributen (onderdelen van de digitale identiteit van de gebruiker) zijn:

- Naam, voornaam,
- Rijksregisternummer,
- Organisatiecode (e.g. KBO-nr)
- Rolleninformatie
- Etc.

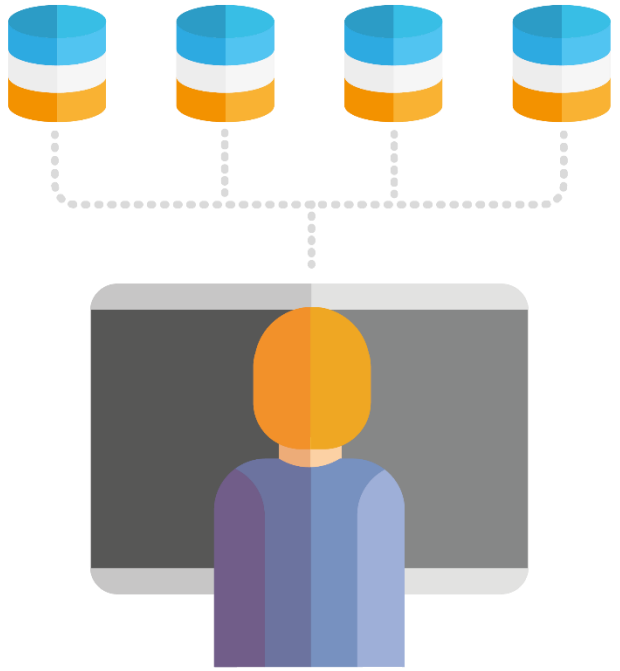
Per toepassing wordt gedefinieerd welke informatie zinvol is (data-minimalisatie), verwerkt mag worden (privacywetgeving en autorisaties privacy-commissie), en beschikbaar is (bron)



Informatie vanuit IDM of andere bron

Aanmeldinformatie wordt gehaald uit:

- Vlaams Gebruikersbeheer (IDM)
- Federale Authenticatie Service (FAS)
- Kruispuntbank Ondernemingen (KBO)
- Beheer der toegangsbeheerders (BTB)
- eHealth (KSZ, niet-standaard)
- Andere specifieke bronnen op aanvraag



Gebruikersbeheer

DIGITAAL VLAANDEREN

Vlaamse overheid

Wat is het Gebruikersbeheer?

Het Gebruikersbeheer (IDM) draait om toegang geven aan gebruikers door hen de juiste rechten toe te kennen

- Waar ACM de 'toegangspoort' naar toepassingen is, kan in IDM het 'toegangsbewijs' aan de eindgebruiker worden verstrekt

IDM stelt beheerders van organisaties in staat hun medewerkers te beheren en rechten te geven voor een toepassing namens hun organisatie, m.a.w. te autoriseren:

- Gebruikers beheren: "Wie werkt er voor mijn organisatie in welke hoedanigheid?"
- Autoriseren: "Piet mag namens ons bedrijf in toepassing X"

IDM maakt grofmazige en fijnmazige toegang tot een toepassing mogelijk via gebruikersrechten:

- Grofmazige autorisatie: "Ik mag namens mijn bedrijf in toepassing X"
- Fijnmazige autorisatie: "Ik mag namens mijn bedrijf in toepassing X als beheerder"

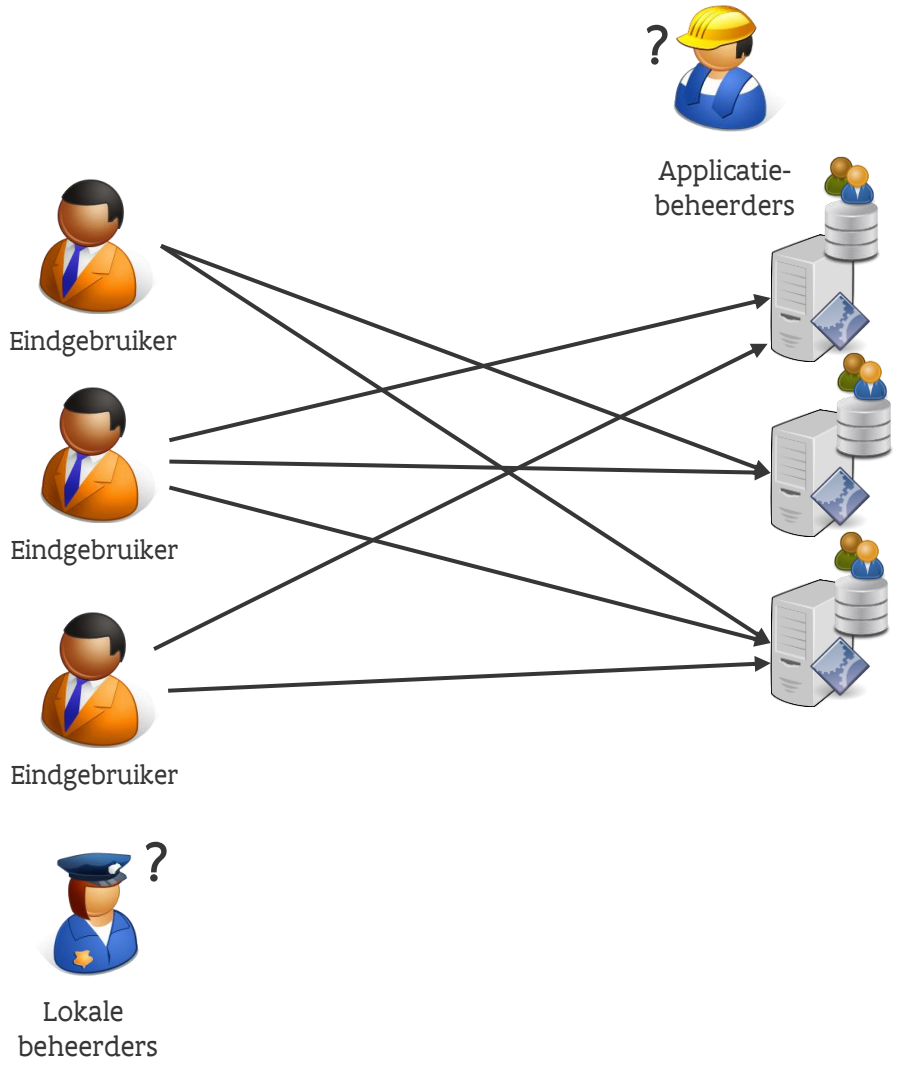
Use cases i.k.v. gebruikers beheren

Niet iedereen mag zomaar binnen in een toepassing, of mag zomaar alles in de toepassing. Toegangsrechten zijn nodig

Vaak worden rechten in de toepassing zelf geregeld., met volgende nadelen

- Gebruikers moeten apart toepassingseigenaren contacteren om rechten te voorzien, te krijgen
- Toestemming van organisatievertegenwoordigers zijn niet gemakkelijk te voorzien
- Organisatievertegenwoordigers hebben geen overzicht wie nu wat mag namens hun organisatie
- Rechten aanmaken neemt veel tijd in beslag en blijven vaak bestaan na vertrek van een medewerker
- Grotere ontwikkel- en beheerskosten omdat de rechten ingebed zijn in de toepassing

Toepassingseigenaren moeten telkens zelf de nodige (kostbare) componenten voorzien

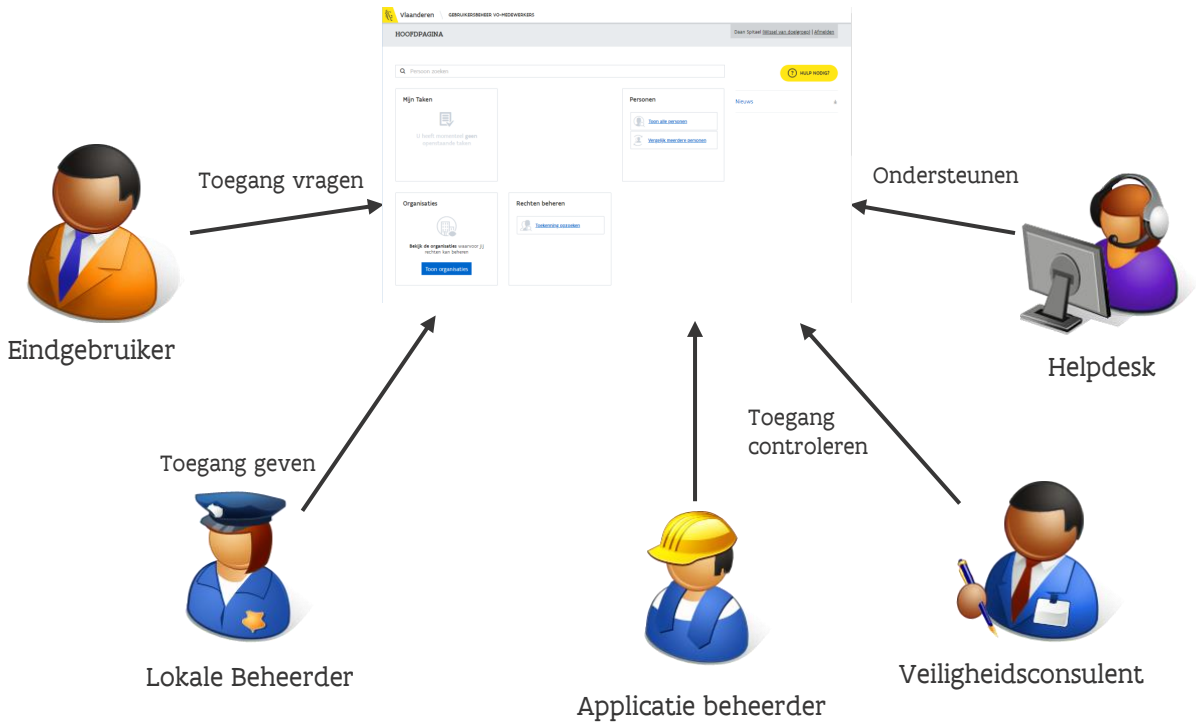


DIGITAAL VLAANDEREN

Vlaamse overheid

De oplossing via IDM - Gebruikersbeheer

- IDM biedt de oplossing om makkelijk en veilig gebruikers en hun gebruikersrechten voor online toepassingen en informatie te beheren
- IDM beheert alle gebruikersrechten op 1 plaats, over de verschillende aangesloten Vlaamse toepassingen heen
- Elke belanghebbende meldt aan op het centrale platform in de juiste hoedanigheid, om toegang te geven en gebruikers te beheren, rechten te controleren of gebruikers te ondersteunen
- IDM is gebruiksvriendelijk, privacy-conform, en toegankelijk vanaf het internet (mits de gebruiker ook de nodige rechten heeft)



Vlaamse overheid

Gedelegeerd beheer als basisprincipe

Het belangrijkste principe van IDM is dat van 'gedelegeerd beheer': het zijn aangewezen personen binnen de organisaties zelf die gebruikers en rechten beheren.

- Met andere woorden, niet de toepassingseigenaren of de bouwsteeneigenaar (ACM/IDM-team) beheren de rechten. Tijdens de integratie bepaalt de toepassingseigenaar wel wat de doelgroep is en welke organisaties (potentieel) toegang mogen krijgen.

Gedelegeerd beheer maakt zelfbeheer in real time mogelijk: lokale beheerders kunnen zelf direct gebruikers beheren en rechten uitdelen zonder tussenkomst van een derde.

Het zijn de lokale beheerders die de verantwoordelijkheid dragen voor de bevestiging dat een gebruiker bij hem werkt en acties namens de organisatie mag uitvoeren in de toepassing.

- Interne processen dienen te worden voorzien voor nieuwe of vertrekkende medewerkers, en nazicht van rechten.

Er kunnen één of meerdere lokale beheerders zijn per organisatie:

- Bijvoorbeeld voor het Lokaal bestuur, onderneming of school

De lokale beheerder wordt altijd aangeduid door de juridisch verantwoordelijke:

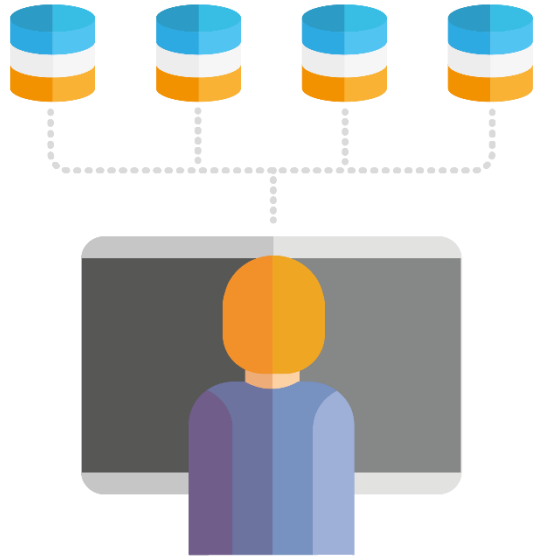
- Secretaris (voor gemeente)
- Wettelijke vertegenwoordiger in KBO (i.s.m. "Beheer der Toegangsbeheerders")
- Inrichtende macht

Lokale Beheerder

Andere bronnen lezen of vullen vanuit IDM

Indien een andere bron moet gelezen of gevuld worden vanuit IDM, gaan we na of dit via een standaardservice kan verlopen (bv. SCIM protocol)

Indien een standaardintegratie niet mogelijk is, bekijken we samen de behoeften/noden voor een niet-standaard integratie (zal via offerte verlopen, niet kosteloos)



Zelfregistratie

Eindgebruikers kunnen zelf ook het initiatief nemen om een gebruikersrecht aan te vragen bij hun lokale beheerder

- Dient te worden geconfigureerd

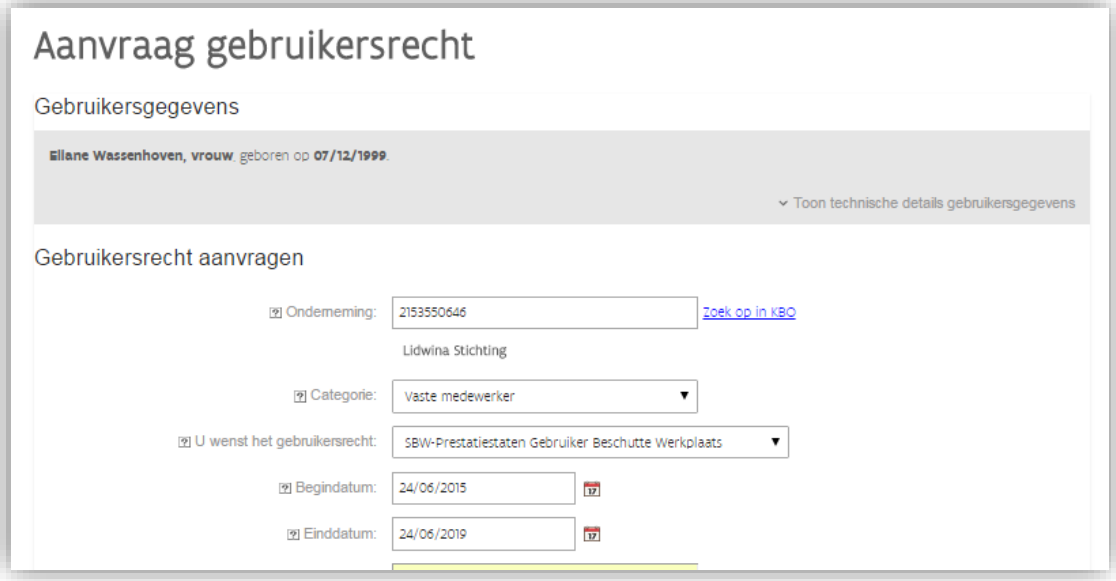
Identificatie gebeurt via ACM

- Dit voorkomt het uitwisselen van rijksregisternummer
- Formulier vraagt geen info die al gekend is

Toepassingseigenaars kunnen de zelfregistratiefunctie gebruiken door de specifieke URL samen te stellen en in te bouwen

- Bijvoorbeeld op landingspagina van toepassing in te bouwen

Zie ook de Zelfregistratie-presentatie.



DIGITAAL VLAANDEREN

Vlaamse overheid

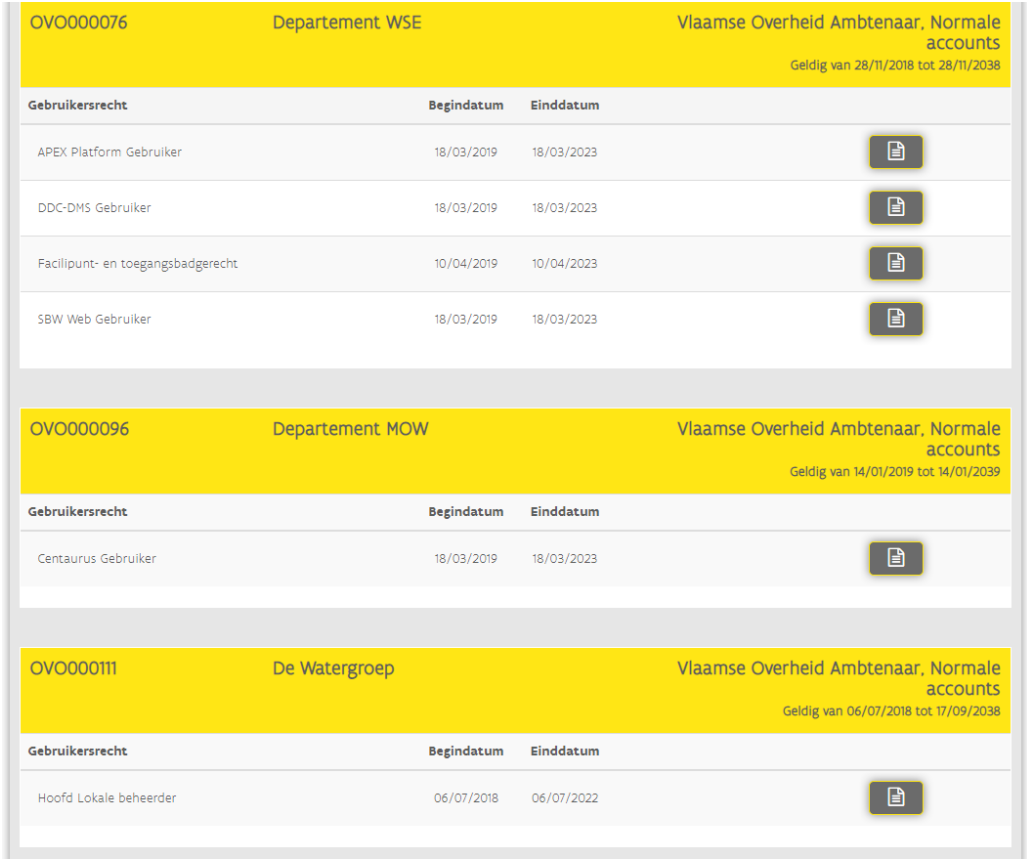
Mijn Profiel voor eindgebruikers

Alle geregistreerde gebruikers in het Gebruikersbeheer hebben een profielpagina

- Laat alle werkrelaties en rechten zien voor de gebruiker
- Laat alle toegangsrechten zien op de werkrelaties
- Laat zien wie de lokale beheerders binnen de eigen organisaties zijn

De ‘Mijn Profiel’-pagina ondersteunt daarmee transparantie naar de eindgebruiker

Zie: https://mijnprofiel-gebruikersbeheer.vlaanderen.be



DIGITAAL VLAANDEREN

Vlaamse overheid

Integreren

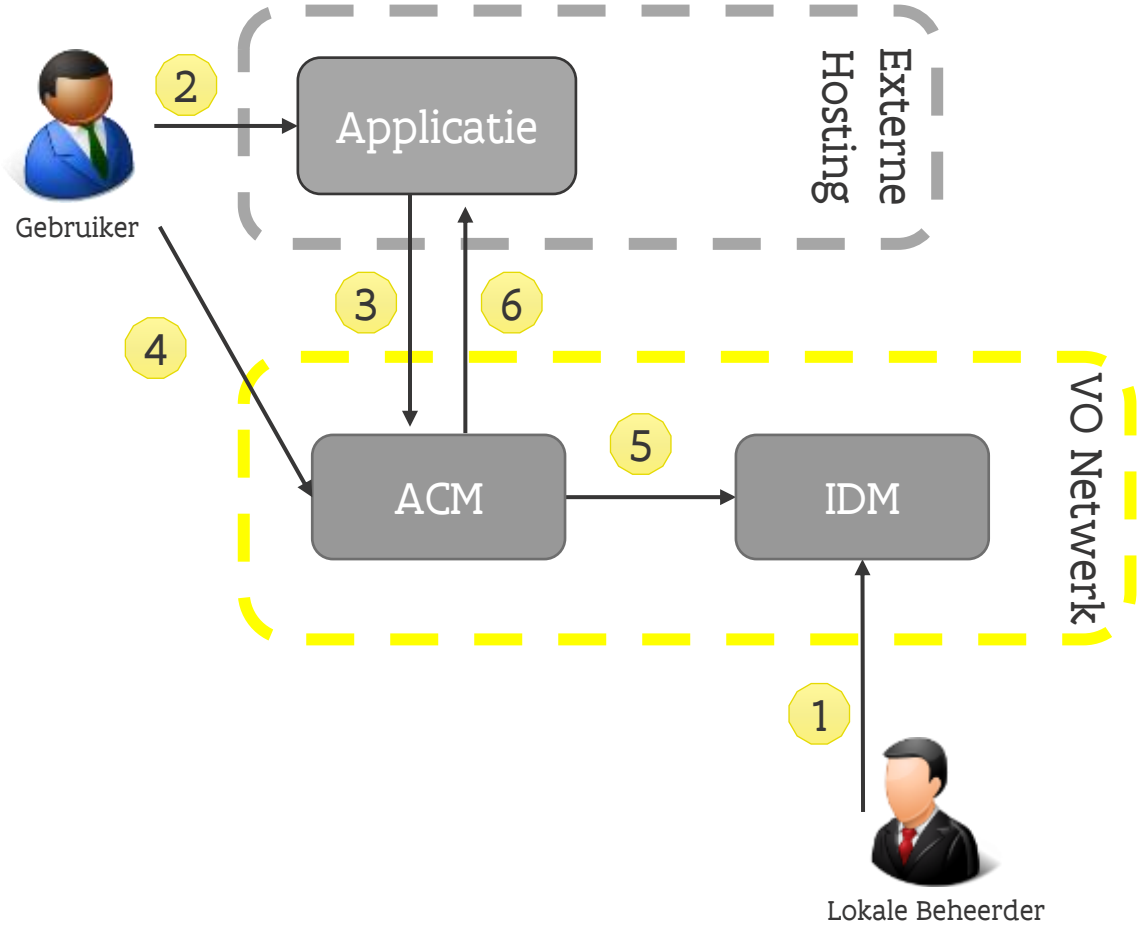
DIGITAAL VLAANDEREN

Vlaamse overheid

Het volledige plaatje

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 in het Gebruikersbeheer,
6. ACM stuurt de autorisatiebeslissing en gebruikersinformatie terug naar de applicatie

De gebruiker is nu ingelogd!



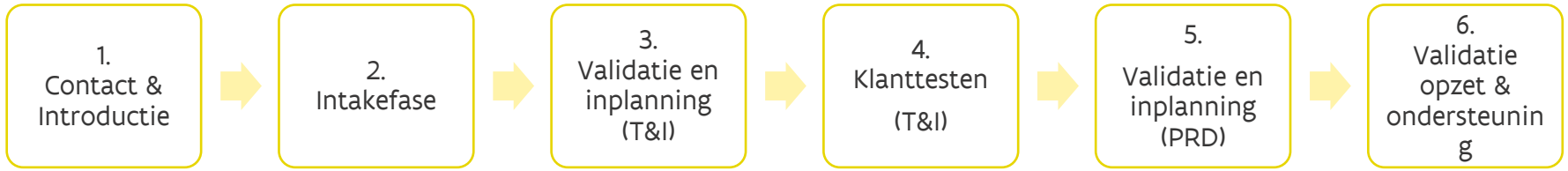
Hoe aansluiten?

Je kan gebruik maken van ACM en IDM door je toepassing(en) aan te sluiten op onze producten. Daarvoor doorloop je samen met ons integratieteam de standaard aansluitingsprocedure

- ACM: technische aansluiting
- IDM: rechtenconfiguratie

Onze analisten begeleiden je door dit proces via een **integratiedossier**, waarin de afspraken en vereisten gedocumenteerd worden. Zowel voor nieuwe dossiers als voor wijzigingen op bestaande dossiers wordt deze procedure doorlopen

Het hele integratieproces (met doorlooptijden) is op onze webpagina terug te vinden



Wat valt binnen de standaard?

- Standaard
  - → Gedelegeerd beheer van gebruikers- en rechten via de online toepassing
  - → Claims based authenticatie via open standaarden
    - × OpenID Connect
    - × OAuth
    - × SAML 2.0
    - × Reverse Proxy (HTTP Headers)
  - → Informatie in standaardformaten
  - → Digitaal Vlaanderen draagt kosten van advies en integratie, klant draagt enkel eigen kosten
  - → Standaarddoorlooptijden van toepassing

Vlaamse overheid

Wat valt niet binnen de standaard?

Niet-standaard

- Provisionering van gebruikers- en rechteninformatie via webservices of exports
- Dynamisch ophalen van rechteninformatie door IDM
- Nieuwe functionaliteiten en overig maatwerk
- Klant draagt kosten van enkel het niet-standaard gedeelte van de integratie
- Doorlooptijden o.b.v. offerte van toepassing

Voorbereiding kennismaking en intake

Tijdens een integratie is het belangrijk zowel de business als de technische kant te betrekken; zorg dus voor een goede voorbereiding met input van beide kanten

De belangrijkste vragen tijdens een intakegesprek zijn onder andere:

- Wat doet de toepassing?
- Voor wie is de toepassing bestemd?
- Wat kunnen en mogen verschillende typen gebruikers (rechtenmodellering)?
- Welke informatie over de gebruikers is nodig?
- Welk integratieprotocol heeft de voorkeur?
- Welke planningsverwachtingen zijn er?
  - Zie ook onze standaarddoorlooptijden; hoe vroeger een eerste gesprek, hoe beter!

Contactinfo
Toegangs- en Gebruikersbeheer

Online:

- http://overheid.vlaanderen.be/gebruikersbeheer
- http://overheid.vlaanderen.be/toegangsbeheer

Mailtje sturen?

- integraties@vlaanderen.be

Ondersteuning via gratis nummer 1700

DIGITAAL VLAANDEREN

Vlaamse overheid