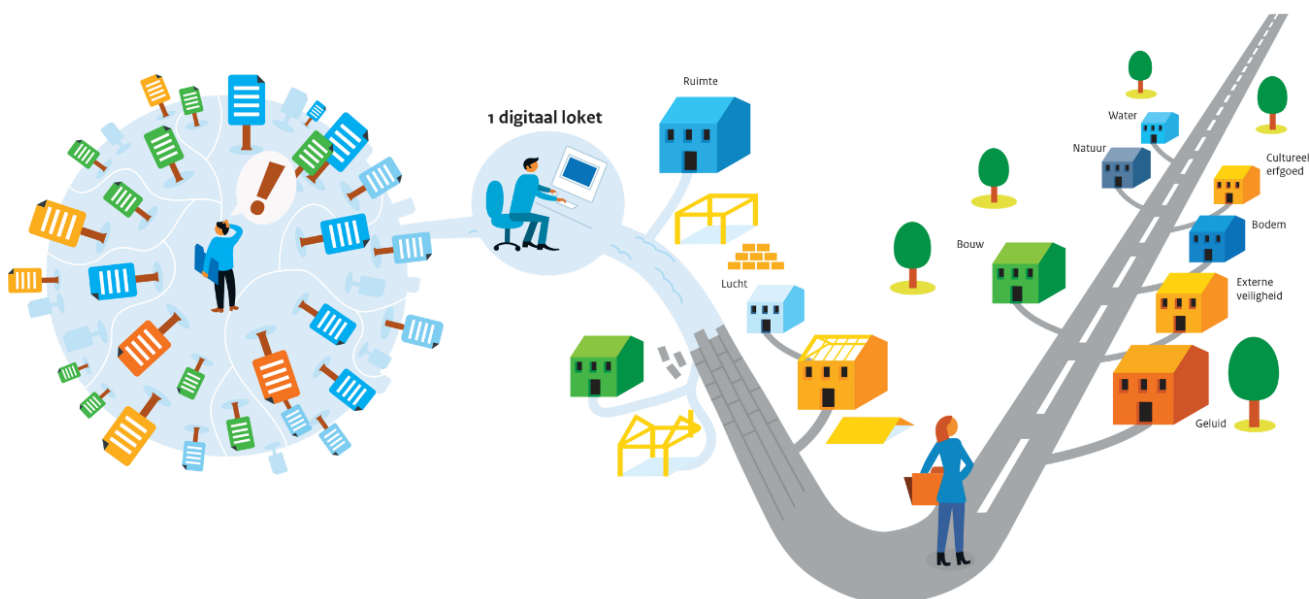


DSO-LV bouwblokken

OGAS - Bijlage E

Version 2.0 • Definitief



Gegenereerd op : 3/18/2020

Auteur(s) : ADSMO

Inhoudsopgave

Eisen aan bouwblokken	4
Positionering	5
Bouwblokken	7
AC01a-E: Platform	8
AC01b-E: Beheer	11
AC01c-E: Privacy & beveiliging	12
AC02-E: Generieke Digitale Infrastructuur (GDI)	14

Deze pagina is opzettelijk leeg gelaten.

Eisen aan bouwblokken

De volgende eisen worden gesteld aan bouwblokken (onderverdeeld in een aantal categorieën):

Architectuur en life cycle management

- Bouwblokken kennen een zelfstandige levenscyclus, zijn separaat beheerbaar, van ontwikkeling tot exploitatie.
- Bouwblokken hebben een leverancier-neutraal koppelvlak. Hierdoor leidt het updaten van een standaard product, waarbij de koppelvlakken gewijzigd zijn, niet direct tot aanpassing van componenten die gebruik maken van het bouwblok. Daarnaast voorkomt het vendor lock-in, zodat het standaard product vervangen kan worden zonder dat componenten die het bouwblok gebruiken aangepast moeten worden.
- Er zijn geen harde afhankelijkheden die portabiliteit in de weg staan.
- Een bouwblok conformeerde zich aan overheidsstandaarden.

Functionaliteit en gebruik

- Functionaliteit van een bouwblok moet op één functie of functionaliteit gericht zijn (dus geen kerstboom). Die specifieke functie moet goed en gefocust worden aangeboden en uitgevoerd. De functionaliteit is helder afgebakend (dus wat wel en niet kan).
- Bouwblokken zijn generiek opgezet en door verschillende partijen te gebruiken in een multi-tenant omgeving. Dit betekent dat in ieder geval ieders gegevens goed afgeschermd zijn.
- Bouwblokken zijn (indien nodig) via internet toegankelijk en worden via services (API's) aangesproken.
- Bouwblokken kunnen eenvoudig aangestuurd worden via een toegesneden API in een reguliere programmeertaal (Java) of op basis van standaard protocol (RESTful, JSON).
- Bouwblokken zijn performant en gebruiken resources optimaal.
- Bouwblokken moeten afgerekend kunnen worden op basis van gebruik (pay per use) per tenant.

Beveiliging

- Bouwblokken kennen een hoge beschikbaarheid.
- Bouwblokken voldoen aan het baseline beveiligingsniveau of kunnen eenvoudig in het regime worden opgenomen.
- Bouwblokken waarbij de identiteit van de gebruiker een rol speelt passen in een identity access management (IAM) framework op basis van standaarden.

Beheer

- Bouwblokken zijn schaalbaar en werpen geen hindernissen op voor de schaalbaarheid van het onderliggende platform.
- Een bouwblok is robuust en bevat handvatten voor foutherstel, terugrollen, schonen, herinjecteren of andere mechanismes om fouten snel en integer te kunnen oplossen.
- Er kan worden gekoppeld met standaard monitoring en alerting frameworks.
- Er wordt voldoende en to-the-point loginformatie opgeslagen voor de beheerbaarheid.
- Bouwblokken hebben eigen webgebaseerde beheerfunctionaliteiten. Deze zijn via internet toegankelijk.
- Een bouwblok is on-demand beschikbaar, eenvoudig installeerbaar en zelfstandig gepackaged.
- Er zijn versies van de bouwblokken om de gehele OTAP straat te kunnen doorlopen. Voor OT zijn er stubs aanwezig waar nodig.
- Beheren (toevoegen, aanpassen en verwijderen) kan volledig via zelfbediening worden geregeld.

Documentatie

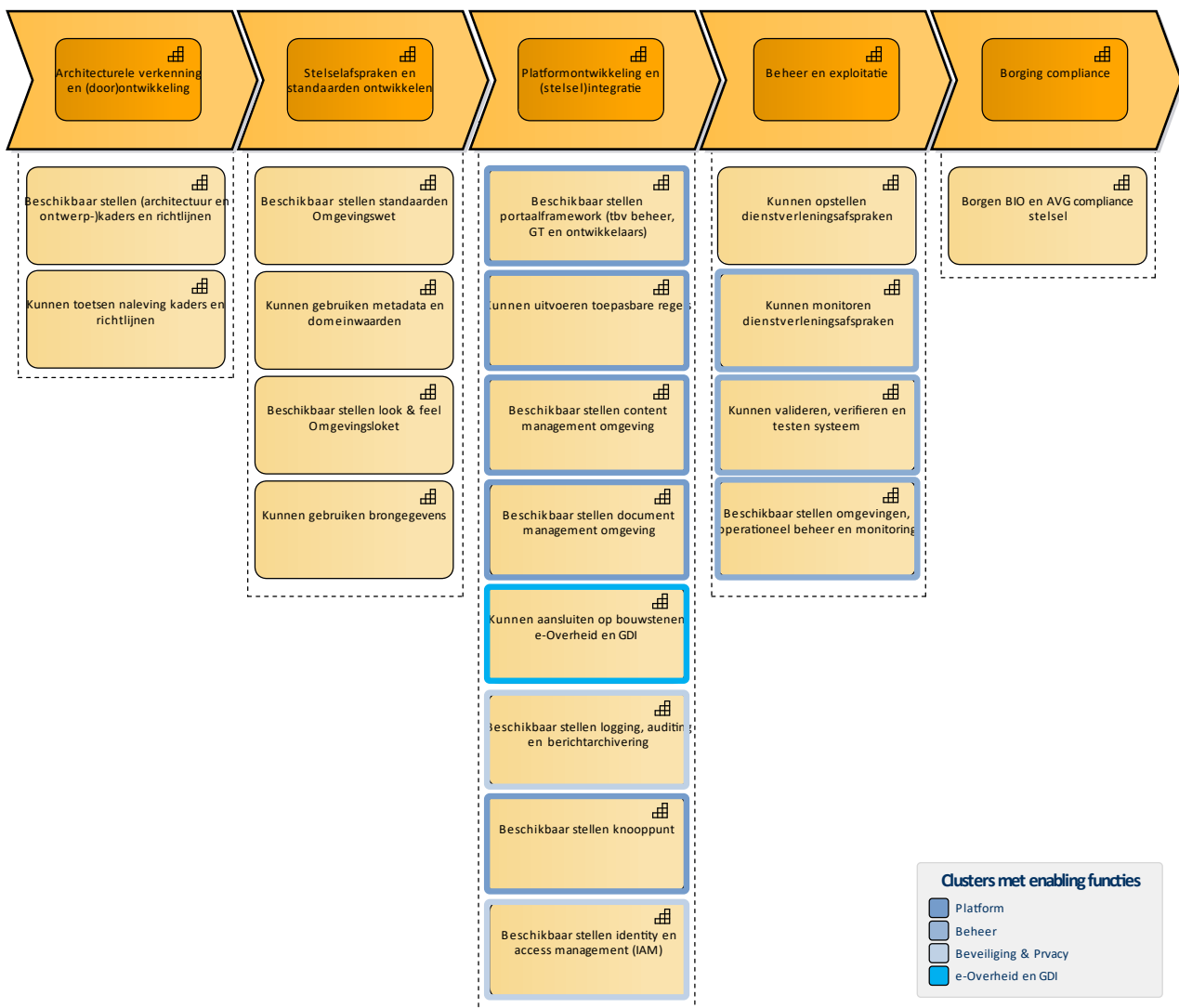
- Bouwblokken zijn goed gedocumenteerd zodat voor de ontwikkelaar en functioneel beheerder helder is hoe deze te beheren en te gebruiken zijn.
- Kwaliteitskenmerken, QoS, SLA, Support en kosten zijn goed beschreven en onderdeel van de oplevering van een bouwblok.

Intellectueel eigendom

- Een bouwblok is rechtenvrij of kan met de juiste toestemming gedurende de volledige lifecycle gebruikt worden.
- De broncode is beschikbaar om onafhankelijk van de oorspronkelijke ontwikkelaar in noodgevallen incidenten te kunnen oplossen en de mogelijkheid voor eigen doorontwikkeling open te houden.

Positionering

Een groot gedeelte van de enabling-capabilities wordt ondersteund door enabling-functies. Deze zijn onderverdeeld in vier clusters. In ieder van deze clusters worden verschillende bouwblokken toegepast. Een bouwblok is een stuk afgebakende generieke functionaliteit dat geheel is toegespitst op de specifieke toepassing. Als een bouwblok niet beschikbaar is wordt deze bij voorkeur op basis van bestaande software eenmalig gerealiseerd voor het stelsel en hergebruikt door andere stelselcomponenten.



Figuur 1 - Toedeling van enabling-functies (in vier clusters)

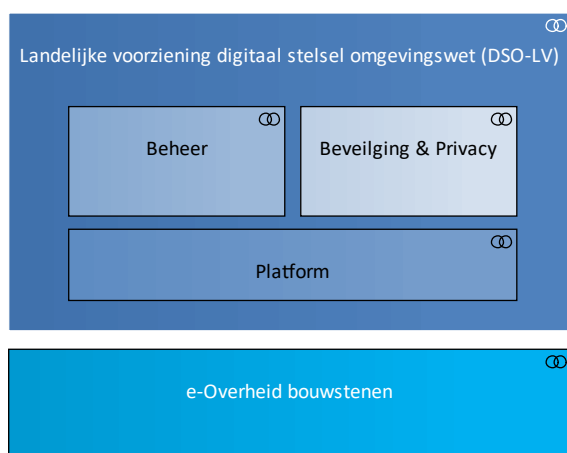
Een bouwblok is per definitie bedoeld om meervoudig (in meerdere situaties) in te zetten en moet daarom in de kern herbruikbaar zijn. De functionaliteit is ondersteunend aan specifieke businessfunctionaliteit (enabling) en kan daarom generiek van opzet zijn.

Deze pagina is opzettelijk leeg gelaten.

Bouwblokken

De bouwblokken zijn als infra-diensten gedefinieerd en worden beschouwd als enabling-functies met één of meerdere onderliggende implementatie(s). De enabling-functies zijn gepositioneerd in vier clusters, waarvan er drie binnen DSO-LV vallen:

- **Platform**
- **Beheer**
- **Privacy en beveiliging**
- **Generieke Digitale Infrastructuur (GDI)**



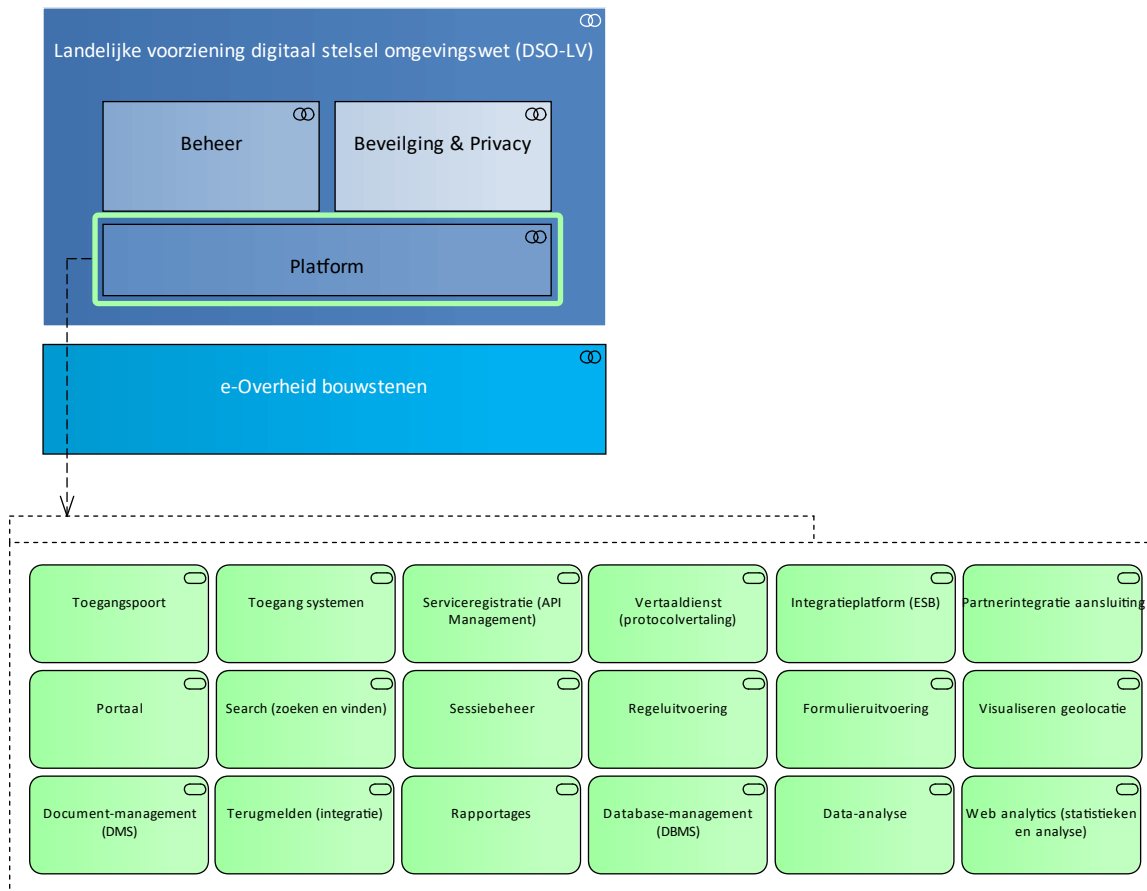
Figuur 2 - clusters met infradiensten

In de onderstaande tabel worden de vier clusters toegelicht. In hoofdstuk 5 van de OGAS wordt ook de relatie met de enabling capabilities en de applicatieclusters van DSO-LV beschreven.

#	Enabling-functies	Toelichting
AC01a-E	Platform	Generieke applicatiediensten van het beschikbaar gestelde platform, waaronder een sessiemanager, zoekmachine, JavaScript-engine, centraal aansluitpunt, rule-engine, CMS en DMS.
AC01b-E	Beheer	Generiek beheerdiensten van de beheervoorziening, waaronder infra- en knooppunt-monitoring en infrarapportage.
AC01c-E	Privacy & beveiliging	Generieke diensten gericht op privacy en beveiliging van het beschikbaar gestelde platform, waaronder een gebruikersgegevensservice (GGS), Identity Server, aansluiting op externe registraties COR en KvK, auditing, log-frameworks en een berichtarchief.
AC02-E	e-Overheidsbouwstenen	Generieke diensten van de overheid in de breedste zin, waaronder PDOK, RDNAPTRANS, externe registers en basisregistraties, berichtenboxen, elektronische authenticatie-middelen zoals e-Herkenning, DigiD en eIDAS.

AC01a-E: Platform

In dit hoofdstuk wordt beschreven welke bouwblokken in het Platform-cluster een rol spelen. Daarnaast wordt per bouwblok aangegevens welke onderliggende implementie(s) worden toegepast.



Figuur 3 - Platform-cluster met infradiensten

■ Data-analyse	Implementatie: • Piwik (web-analytics)
<i>Ad hoc data analyse uitvoeren op bepaalde patronen.</i>	
■ Database-management (DBMS)	Implementatie: • PostgreSQL • PostGIS
<i>Opslag voor gestructureerde en GEO gegevens.</i>	
■ Document-management (DMS)	Implementatie: • Alfresco
<i>Ongestructureerde gegevensopslag voornamelijk voor documenten.</i>	
■ Documentgeneratie	Implementatie: • Jasper Reports
<i>Geeft opmaak aan XML document en maakt daar een pdf van.</i>	

Formulieruitvoering

Implementatie:
• React (maatwerk)

Een formulier uitvoeren met het geheel van vragen en antwoorden dat door een gebruiker ingevuld moet worden.

Integratieplatform (ESB)

Implementatie:
• WSO2-EI

Betrouwbaar uitwisselen van berichten en het uitvoeren van transformaties en translaties.

Partnerintegratie aansluiting

Implementatie:
• Digipoort

Centraal aansluitpunt voor bedrijven naar overheid.

Portaal

Implementatie:
• AngularJS (maatwerk)

Portaalfunctie waarin gebruikerstoepassingen worden geïntegreerd.

Rapportages

Implementatie:
• Jasper Reports

Rapportagetool voor eindgebruikers, zoals business analisten en functioneel beheerders.

Regeluitvoering

Implementatie:
• Drools

Rule engine die beslisbomen met executeerbare regels uitvoert om een gebruiker door vragen heen te leiden om te bepalen of de wet- en regelgeving van toepassing is.

Search (zoeken en vinden)

Implementatie:
• Elasticsearch

Generieke zoekfunctie.

Serviceregistratie (API Management)

Implementatie:
• WSO2 API Manager

Centrale registratie en beheer van de omgevings specifieke configuraties van applicaties, beheer van webservices en geautomatiseerd uitrollen van applicaties.

Sessiebeheer

Implementatie:
• Sessiemanager (maatwerk)

Bijhouden en beschikbaar maken van sessieinformatie na inloggen (n.b. nu geen standaard portal oplossing wordt gekozen wordt dit maatwerk en geen bouwblok meer maar maatwerk).

Terugmelden (integratie)

Implementatie:
• Federatieve terugmeldfunctie (in ontwikkeling bij Logius/Kadaster)

Terugmelding via een generieke API naar een systeem voor terugmeldingen, welke de van en naar gemeenten/bronhouders verzorgd, via een portaal.

Toegang systemen

Implementatie:
• PKI Overheid certificaten

Authenticeren van systemen (PKI overheid certificaten).

Toegangspoort

Implementatie:
• API-gateway

Generiek mechanisme om toegang tot systemen op grofmazig niveau te handhaven.

Vertaaldienst (protocolvertaling)

Implementatie:
• ebMS adapter

Protocolvertaling van ebMS naar WUS en andersom.

■ **Visualiseren geolocatie**

Implementatie:

- *Viewer Regel en Kaart*

Gebruikerstoepassing voor het tonen van regels met het werkingsgebied op de kaart

■ **Web analytics (statistieken en analyse)**

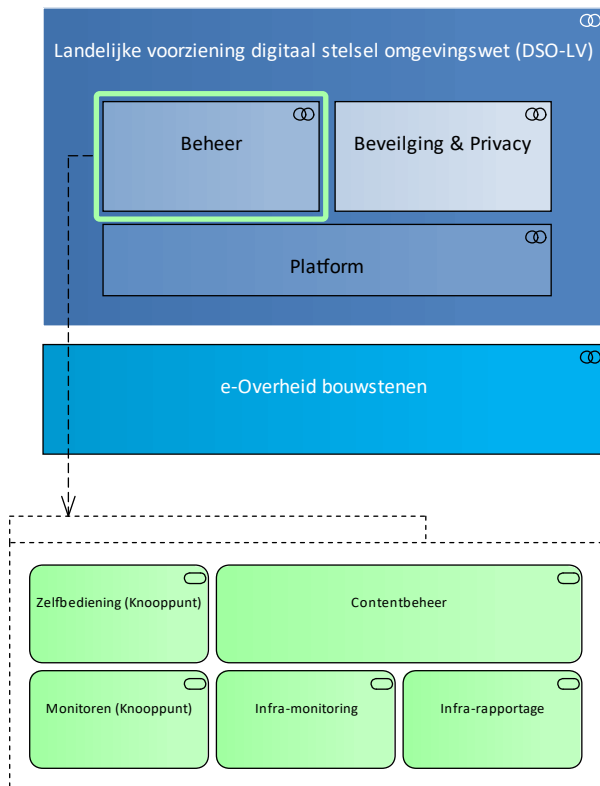
Implementatie:

- *Piwik (web-analytics)*

Analyse en rapportage gebruik webportaal.

AC01b-E: Beheer

In dit hoofdstuk wordt beschreven welke bouwblokken in het Beheer-cluster een rol spelen. Daarnaast wordt per bouwblok aangegevens welke onderliggende implementie(s) worden toegapast.



Figuur 4 - Beheer-cluster met infradiensten

Contentbeheer

Implementatie:

- IPROX CMS

Beheren van content (teksten, afbeeldingen en video) van o.a. front-end maar ook andere stelselonderdelen.

Infra-monitoring

Implementatie:

- Prometheus (monitoring)

Monitoren van de gezondheid van infrastructuur (netwerk, hardware en opslag), applicaties en webservices.

Infra-rapportage

Implementatie:

- Grafana (rapportage)

Rapporteren over de kwaliteit van de dienstverlening van applicaties en componenten.

Monitoren (Knooppunt)

Implementatie:

- Prometheus (monitoring)

Registreren en presenteren van gebruiksstatistieken van applicaties en berichtenverkeer.

Zelfbediening (Knooppunt)

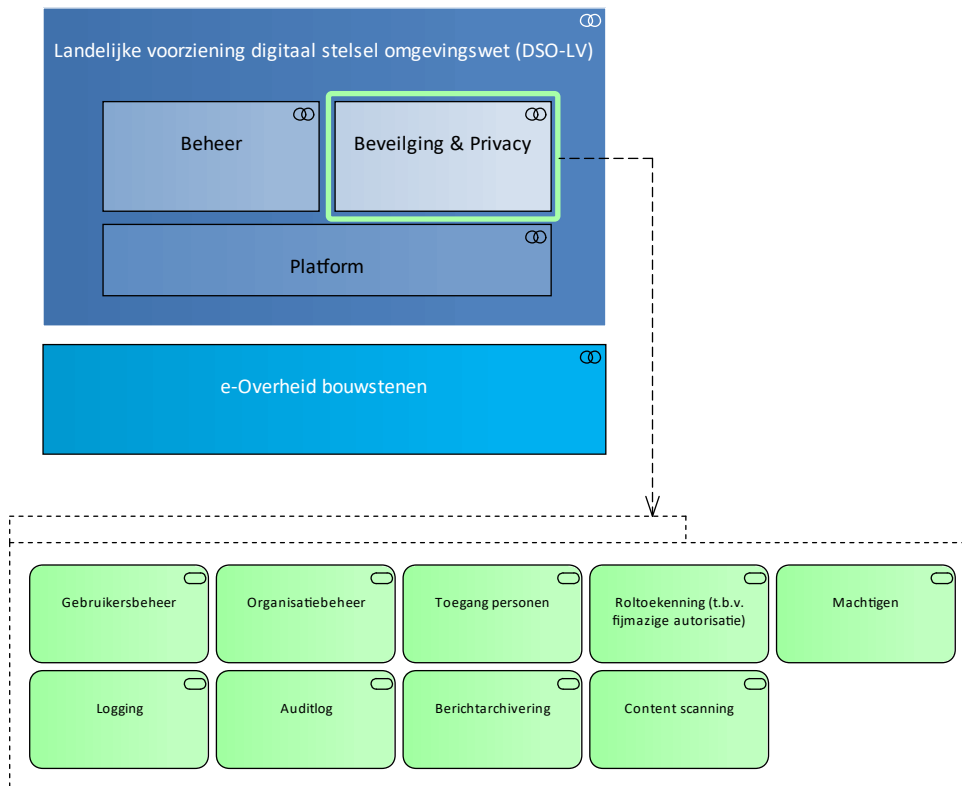
Implementatie:

- WSO2 API Store

Portaal waarin aanbieders en afnemers het gebruik van services op het centraal aansluitpunt zelf kunnen registreren, configureren en uitrollen met minimale betrokkenheid van de beheer organisatie.

AC01c-E: Privacy & beveiliging

In dit hoofdstuk wordt beschreven welke bouwblokken in het Privacy & beveiliging-cluster een rol spelen. Daarnaast wordt per bouwblok aangegevens welke onderliggende implementie(s) worden toegepast.



Figuur 5 - Privacy & beveiliging-cluster met infradiensten

Auditlog	Implementatie: • <i>Auditing (maatwerk)</i>
Vastlegging van gebeurtenissen en mutaties inclusief bijbehorende informatie. (conform H10.10 BIR)	
Berichtarchivering	Implementatie: • <i>Berichtarchief (maatwerk)</i>
Vastlegging van alle archiefwaardige berichten die stelsel in- en uitgaan via knooppunt.	
Content scanning	Implementatie: • <i>ClamAV</i>
Generiek mechanisme voor scannen van content op virussen, malware, etc.	
Gebruikersbeheer	Implementatie: • <i>Gebruikergegevensservice (GGS)</i>
Gebruikersgegevens en instellingen onafhankelijk van systemen die deze gegevens gebruiken beheren.	
Logging	Implementatie: • <i>Log-frameworks</i>
Vastlegging van (technische) loginformatie uit de stelselcomponenten.	

Machtigen**Implementatie:**

- Logius Machtigen

Inloggen als gemachtigde en de daarbij behorende machtigingen op informatie-objecten applicatie-onafhankelijk beheren.

Organisatiebeheer**Implementatie:**

- Extern (integratie COR, Kvk)

Organisatiegegevens en instellingen onafhankelijk van systemen die deze gegevens gebruiken beheren.

Roltoekenning (t.b.v. fijnmazige autorisatie)**Implementatie:**

- Knooppunt (rolafleidinggegevens)

Generiek mechanisme voor RBAC (Role Based Access Control) als ABAC (Attribute Based Access Control) op te lossen. Dit is een neutraal koppelvak voor zowel DigiD als eHerkenning.

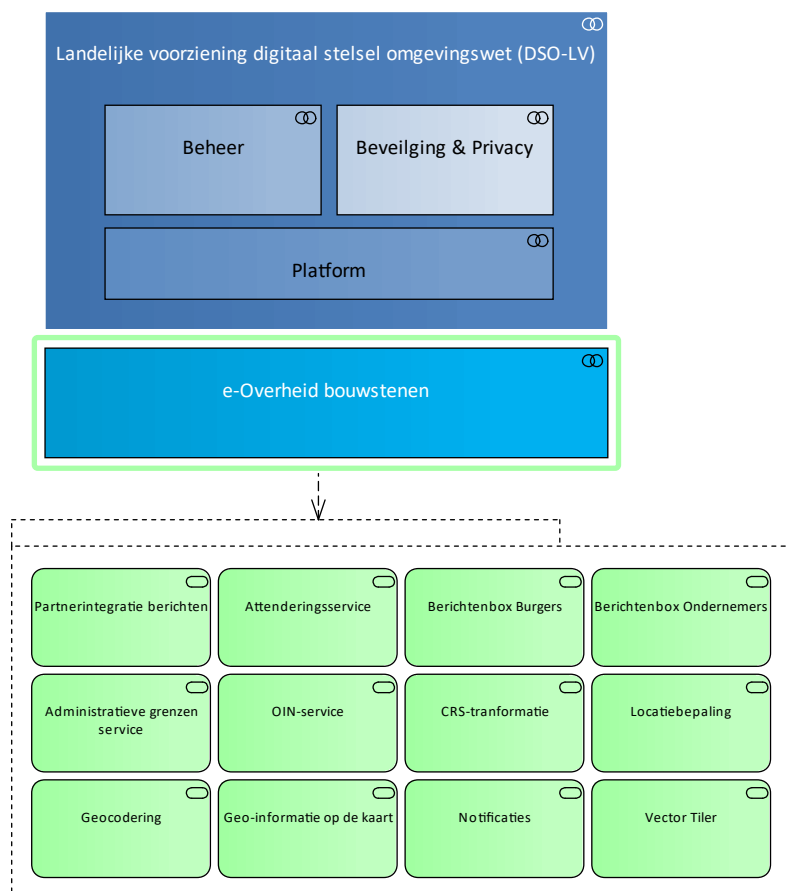
Toegang personen**Implementatie:**

- eHerkenning
- DigiD
- Derdenmiddel
- DigiD SSO
- eIDAS

Component voor het authentifieren van burgers (ingezetenen en niet-ingezetenen) en medewerkers.

AC02-E: Generieke Digitale Infrastructuur (GDI)

In dit hoofdstuk wordt beschreven welke bouwblokken in het Generieke Digitale Infrastructuur (GDI)-cluster een rol spelen. Daarnaast wordt per bouwblok aangegevens welke onderliggende implementie(s) worden toegepast.



Figuur 6 - GDI-cluster met infradiensten

Administratieve grenzen service

Implementatie:

- *Ambtsgrenzen service*

Attenderingsservice

Implementatie:

- *Lokale Bekendmakingen (Mijnoverheid)*

Veel overheden publiceren hun bekendmakingen als serviceproduct op internet. Dit doen zij naast de formele bekendmaking in het huis-aan-huisblad. Een prima manier maar de zoekmogelijkheden zijn over het algemeen erg beperkt. Het is bijvoorbeeld niet mogelijk te zoeken op postcode. Onderzoek wijst uit dat mensen vooral geïnteresseerd zijn in activiteiten vlak bij huis. De attenderingsservice Berichten over uw buurt (voorheen Bekendmakingen) zorgt hiervoor. Iedereen kan een persoonlijk profiel aanmaken en aangeven in welke bekendmakingen ze geïnteresseerd zijn.

Berichtenbox Burgers

Implementatie:

- *Berichtenbox Burgers (Mijnoverheid)*

Hier kan een burger zien wat er geregistreerd is over deze burger bij de overheid, berichten van de overheid ontvangen en overzicht houden over lopende zaken met de overheid.

Berichtenbox Ondernemers**Implementatie:**

- Berichtenbox Ondernemers

Hiermee wisselt een bedrijf digitaal berichten uit met overheidsorganisaties.

CRS-tranformatie**Implementatie:**

- RDNAPTRANS

Geo-informatie op de kaart**Implementatie:**

- PDOK Viewer

Maakt geo data van de Nederlandse overheid eenvoudig toepasbaar als kaartfunctionaliteit in een webpagina.

Geocodering**Implementatie:**

- PDOK Geocoding

De geocodeerdienst maakt het mogelijk om coördinaten om te zetten naar een locatie of een locatie om te zetten naar coördinaten.

Locatiebepaling**Implementatie:**

- PDOK Locatie Server

Bepalen van de locatie met behulp van PDOK

Notificaties**Implementatie:**

- Digikoppeling

Versturen van notificaties.

OIN-service**Implementatie:**

- Centraal OIN Register (COR)

Partnerintegratie berichten**Implementatie:**

- Berichtenkanaal Bevoegd Gezag

Berichten bij bevoegd gezag afleveren.

Vector Tiler**Implementatie:**

- PDOK Vector Tiling

De Vector Tiler vertaalt brongeometrieën (GML) naar vector tiles en maakt deze bevroegbaar via een afnamekoppelvlak.