Drechtsteden

In opdracht van	Ronald Mons (CIO)
Status	Concept
Versie	0.91
Auteur	Dennis de Wit
Datum	30 september 2019

Versiebeheer

Versie	Datum	Wijzigingen	Auteur
0.1	27-06-2019	Eerste versie	Dennis de Wit
0.9	15-07-2019	Definitieve versie op basis van interne afstemming en resultaten uit PoC's	Dennis de Wit
0.91	30-09-2019	Review/aanvullingen verwerkt	Dennis de Wit

Inhoudsopgave

1 Inleiding

1.1 Organisatie

Vanuit de gedachte dat de dienstverlening aan burgers en bedrijven de primaire taak is van de gemeenten en dat het in het belang is van de kwaliteit en continuïteit van de ondersteunende taken als deze op regionaal niveau worden georganiseerd, besloten de gemeenten Zwijndrecht, Papendrecht, Alblasserdam, Hendrik-Ido-Ambacht, Dordrecht en Sliedrecht begin 2006 tot een nauwe samenwerking en de beleids- en uitvoeringstaken te bundelen betreffende de middelenfuncties (waaronder ICT) in een eigen gemeenschappelijke regeling: de Gemeenschappelijke Regeling Drechtsteden (GRD).

De GRD bestaat uit het Servicecentrum Drechtsteden (SCD), het Ingenieursbureau Drechtsteden (IBD), Bureau Drechtsteden (BRD), Gemeentebelastingen en Basisinformatie Drechtsteden (GBD), het Onderzoekscentrum Drechtsteden (OCD) en de Sociale Dienst Drechtsteden (SDD). Deze samenwerking, waar inmiddels een zevende gemeente (namelijk Hardinxveld-Giessendam) aan toegevoegd is, maakt een gemeenschappelijke en gestandaardiseerde infrastructuur noodzakelijk.

1.2 Aanleiding

Door de toenemende hoeveelheid data in de huidige maatschappij wordt Gemeenschappelijke Regeling Drechtsteden in haar bedrijfsvoering steeds meer afhankelijk van data. De huidige werkwijze waarbij de data versnipperd over het landschap in silo's opgeslagen ligt levert tal van knelpunten op.

Data (en ook functionaliteit) wordt in toenemende mate beschikbaar gesteld via API's (Application Programming Interfaces), hierdoor kan gegevensuitwisseling eenvoudig mogelijk gemaakt worden en kunnen silo's verdwijnen. Wereldwijd is deze ontwikkeling al enkele jaren gaande, voor de overheidsmarkt is het relatief nieuw en staat het in verband met de Common Ground beweging.

Om op de juiste manier om te kunnen gaan met API's zoekt Drechtsteden een oplossing op het gebied van 'API-Management'. Onder API-Management wordt kort door de bocht verstaan:
”API Management is het proces van creëren, publiceren en beheren van API's, in een veilige en schaalbare omgeving.”

In dit document wordt in detail gespecificeerd wat Drechtsteden van API-Management tooling vereist.

1.3 Noodzaak inzet tooling

Natuurlijk handelt Drechtsteden vanuit het verbeteren van de dienstverlening aan burgers, bedrijf, ketenpartners. Om deze dienstverlening zo goed mogelijk vorm te geven is het gebruiken van data en functionaliteit van enorme toegevoegde waarde.

Om voor Drechtsteden API's te kunnen aanroepen of te creëren/publicreren is het noodzakelijk dat er tooling beschikbaar is die hierbij kan ondersteunen. Daarbij is het meest essentiële het efficiënt inrichten van API's, zodat er op een betrouwbare en veilige manier gegevens uitgewisseld kunnen worden, in een Cloud-based landschap.
Het huidige instrumentarium van Drechtsteden binnen de Centrale Distributie Voorziening (CDV) schiet hierin tekort (zie verdere details in paragraaf 2.2 Informatie architectuur).

Hieronder worden de onderliggende business drivers voor API-Management kort toegelicht.

Als GRD wil ik het consumeren van data stimuleren

- Door data te consumeren ontstaat informatie, kennis en/of waarde (data driven), waardoor de klant het best bediend kan worden.
- Digitale transformatie: Data moet in een keten eenvoudig te benaderen zijn zodat het ook daadwerkelijk gebruikt kan worden (ook buiten de grenzen van de organisatie bijvoorbeeld voor ketenpartners).

Als GRD wil ik beschikken over goed beveiligde en beheerde gegevensverbindingen

API-Management tooling bevat functionaliteit voor:

- het realiseren van gegevensverbindingen
- het beveiligen van verbindingen
- het inrichten van gegevensautorisatie
- het loggen van datastromen

Als GRD wil ik de kosten voor het realiseren van gegevensverbindingen reduceren

- Data duplicatie kost veel geld en kan slechte datakwaliteit opleveren. Data dupliceren betekent dat data op tal van plekken in de organisatie opgeslagen ligt en beheerd moet worden, in zogenaamde silo's. Met name het beheer van data is tijdrovend (opslag van data wordt momenteel steeds goedkoper) en het niet-real time dupliceren van data levert duplicaten op die niet actueel zijn. "Data ophalen bij de bron" is daar een antwoord op. Dit betekent dat er meer minimalistische (conform doelbinding) real-time gegevensverbindingen tussen applicaties zullen ontstaan, maar dat er minder onnodige data getransporteerd wordt in onzichtbare hoeken van de organisatie.
- Steeds meer applicaties in het landschap van Drechtsteden bevinden zich niet meer on-premise (op het GRID-netwerk). Het realiseren van verbindingen met de buitenwereld kent momenteel een flinke doorlooptijd (en is daarmee kostbaar) aangezien de juiste tooling hiervoor niet aanwezig is. Door de verdergaande ontwikkeling van Cloud moet Drechtsteden hierop voorsorteren.

Als GRD wil ik conform Wet- en Regelgeving om kunnen gaan met data.

- Privacy: Voldoen aan privacywetgeving (AVG), we willen weten bij welke verwerking (proces) welke gegevens gebruikt worden.
- Beveiliging: de juisten maatregelen treffen om risico's te mitigeren.
- Transparantie: voldoen aan richtlijnen Wet Open Overheid (WOO).

Als GRD wil ik aansluiten op lokale, landelijke en wereldwijde ontwikkelingen

Verschillende ontwikkelingen bieden mogelijkheden om gegevensuitwisseling te optimaliseren en de silo's te verwijderen. De toegevoegde waarde daarvan wil Drechtsteden benutten.

- In lijn met de Common Ground beweging
- Ondersteuning van REST/JSON API's
- Aansluiting op NLX[1]
- Geoptimaliseerd voor Cloud-integratie
- Verbindingen mogelijk met Landelijke voorzieningen zoals DSO
- API's maken het mogelijk om functionaliteit t.a.v. A.I. en Blockchain te benutten.

[1] Het is nog niet duidelijk of NLX een product wordt of een voorbeeldimplementatie blijft.

2 Architectuur

In dit hoofdstuk wordt aandacht besteed aan de positionering van de API-Management tooling in de architectuur van Gemeenschappelijke Regeling Drechtsteden, daarnaast worden enkele architectuurrichtlijnen benoemd die Drechtsteden hanteert en die niet specifiek in de requirements van hoofdstuk 3 terugkomen.

2.1 Business architectuur

In hoofdstuk 1 is al uitgebreid beschreven wat de noodzaak is van de inzet van API-Management tooling. Aanvullend hierop wordt het volgende gesteld:

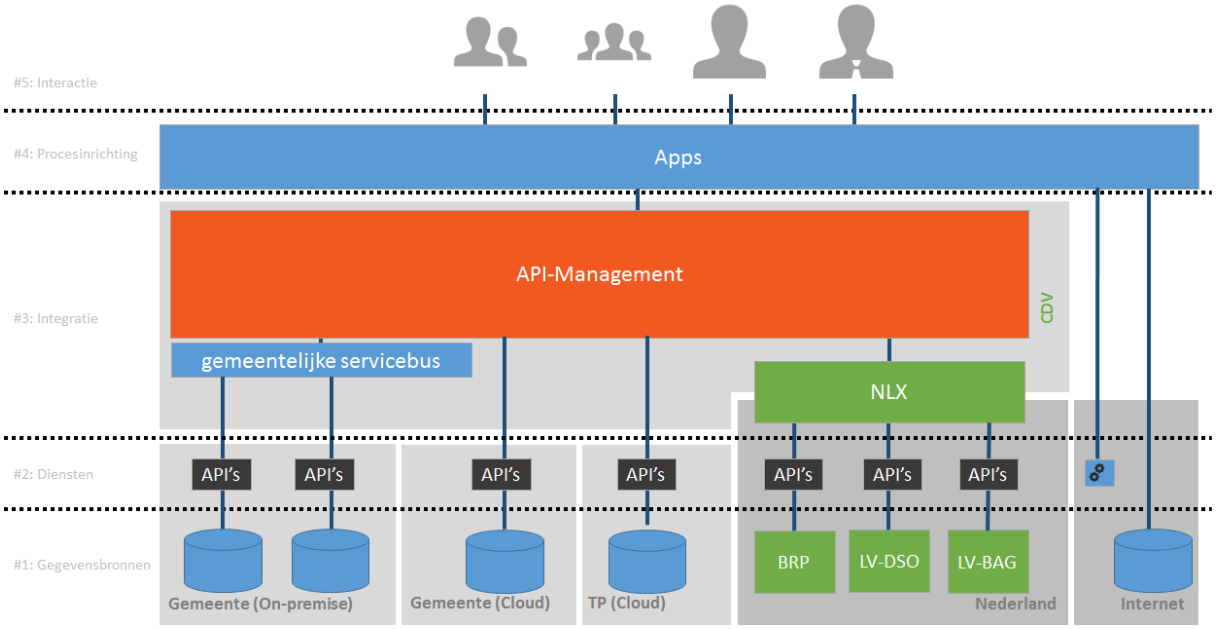
Gebruikers
Binnen paragraaf 2.2 wordt nader onderscheid gemaakt in "API-Management tooling" in referentiecomponenten API-Gateway, API-Manager en API-Portal. Elk referentiecomponent kent een afzonderlijke groep gebruikers.

- API-Gateway: enkel applicaties (consumers en providers van services) gebruiken de gateway. De inrichting ervan vindt plaats via de API-Manager.
- API-Manager: Gebruikers zijn beheerders (zie uiteenzetting beheerwerkzaamheden in hoofdstuk 4).
- API-Portal: Gebruikers zijn medewerkers betrokken of geïnteresseerd in de ontwikkeling en het gebruik van API's. Dit kunnen zowel medewerkers van Drechtsteden zijn, als ook externen (bijvoorbeeld van software leveranciers of ketenpartners).

Producten en diensten
Producten en diensten die worden aangeboden vanuit de API-Management tooling kunnen ook op basis van de referentiecomponenten gespecificeerd worden.
De requirements van de producten en diensten worden in detail beschreven in hoofdstuk 3. Paragraaf 3.1 t/m 3.5 gaat in op de producten en diensten voor de Gateway 3.6 geeft invulling aan de producten en diensten voor het portaal.

2.2 Informatie architectuur

Drechtsteden heeft geruime ervaring met integratievraagstukken. Sinds 5 jaar is er een Drechtsteden-brede integratievoorziening ingericht die invulling geeft aan het faciliteren van gegevensuitwisseling tussen bronnen en afnemers. Binnen Drechtsteden wordt deze centrale voorziening aangeduid als 'Centrale Distributie Voorziening' (CDV).



Figuur 1: Visualisatie 'Positionering API-Management binnen CDV'

De CDV is de gereedschapskist waarbinnen verschillende tools t.a.v. data-integratie zich bevinden. Gezien de wereldwijde ontwikkelingen op het gebied van gebruik van API's ziet Drechtsteden dat de huidige CDV opzet hierin tekort schiet. Dit heeft geresulteerd in het besluit om API-Management tooling aan te schaffen en dit te positioneren binnen de CDV. In figuur 2 is dit gevisualiseerd (de CDV bevindt zich in laag '#3 Integratie').

Rol van gemeentelijke servicebus
Binnen de CDV opereert ook een gemeentelijke servicebus, namelijk Neuron Integratie Platform van leverancier Vicrea. De afgelopen 5 jaar is er veel energie gestoken in het faciliteren van gegevensstromen via de servicebus (met name op basis van StUF). Het is voor Drechtsteden geen doel op zich om bestaande verbindingen te elimineren of de servicebus uit te faseren. De API-Management tooling komt naast de servicebus te staan en gaat aanvullende functionaliteit bieden binnen het CDV-construct.

Wel lijkt gezien de ontwikkelingen in lijn met de visie van Common Ground de aandacht t.a.v. integratievraagstukken te gaan verschuiven van gemeentelijke servicebus naar API-Management tooling. Nieuwe verbindingen zullen vaker gelegd gaan worden via de API-Management tooling en de inzet van de gemeentelijke servicebus wordt teruggedrongen. Enkel op het gebied waar de huidige gemeentelijke servicebus specifieke toegevoegde waarde levert wordt deze voor Drechtsteden nog ingezet voor nieuwe verbindingen (eventueel in combinatie met de API-Management tooling).

Toegevoegde waarde gemeentelijke servicebus:
- StUF-koppelvlakken
- Complexe transformaties

Referentiecomponenten
API-Management tooling omvat de referentiecomponenten API-Gateway, API-Manager en een API-Portal. Hieronder is beknopt beschreven wat Drechtsteden hieronder verstaat.

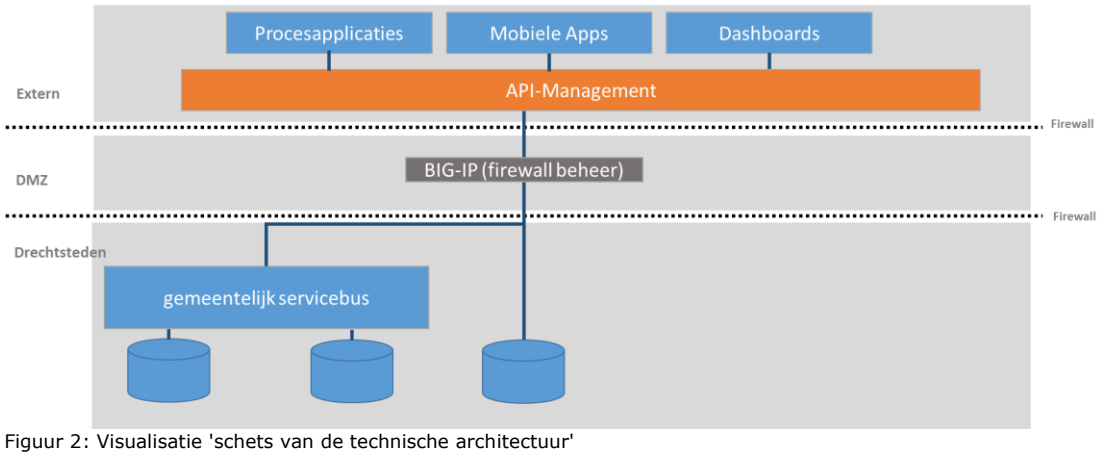
- API-Gateway: de tooling waarmee gegevensverbindingen technisch gefaciliteerd worden.
- API-Manager: de configuratie van de gateway.
- API-Portal: een portaal waarin het dienstenaanbod aan het brede publiek gepresenteerd wordt.

In hoofdstuk 3 zijn per component de requirements in detail beschreven.

2.3 Technische architectuur

Vanuit het beleid van Drechtsteden kan gesteld worden dat:

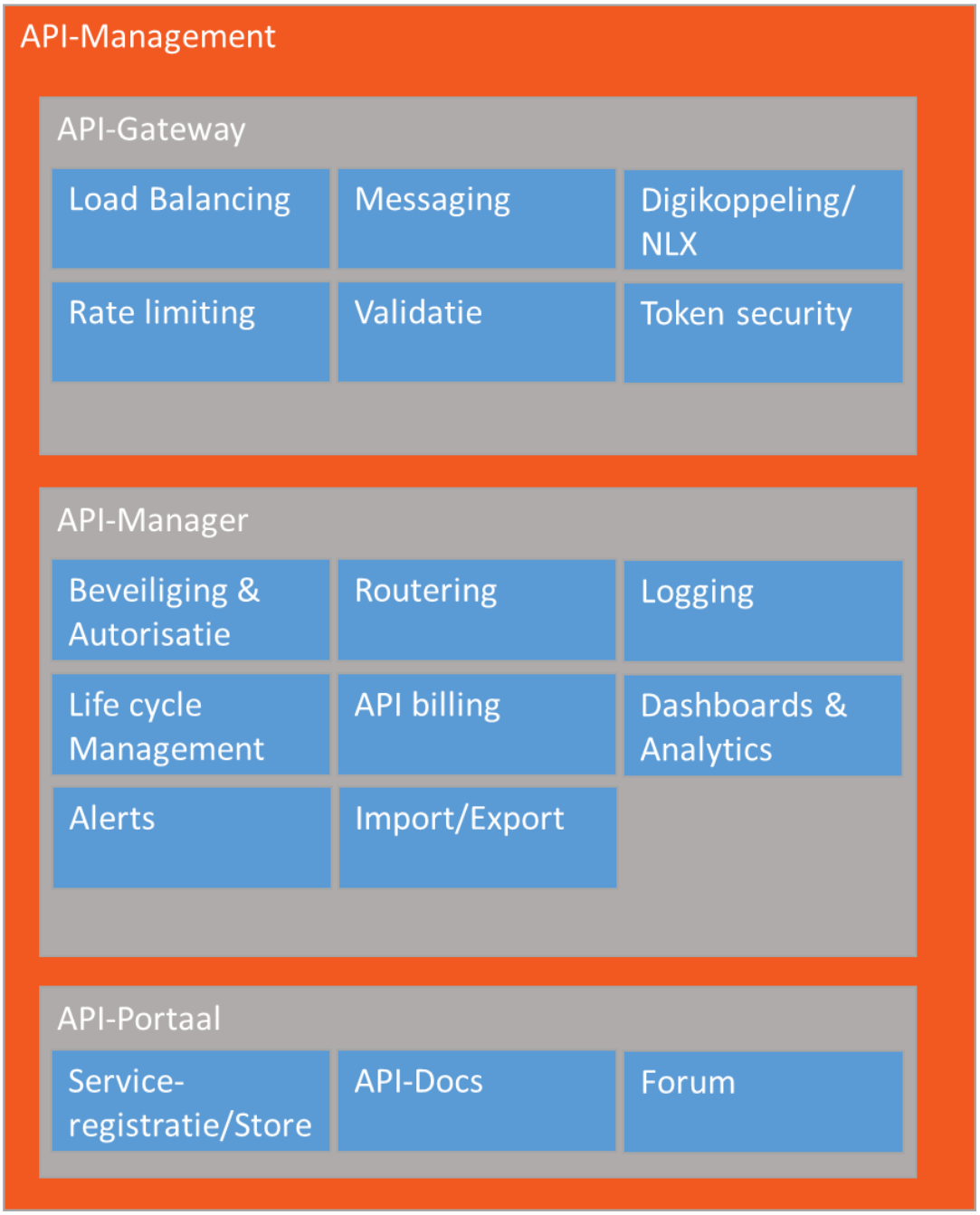
- de API-Management tooling "as a Service" (iPaaS/SaaS) wordt ingezet (bij voorkeur in een shared cloud om de voordelen van grootschalige inzet maximaal te benutten).
- Ook SaaS-2-SaaS verkeer wordt via API-Management tooling ingericht om op die manier gegevensverbindingen te kunnen beheersen.
- Berichtenverkeer dat het Drechtsteden netwerk binnenkomt vanuit buiten verloopt via de reverse proxy BIG-IP (F5). Hierin worden de firewalls geconfigureerd. De API-Management tooling staat niet in het on-premise landschap van Drechtsteden, maar zal wel connectie leggen met on-premise gegevensbronnen. De tooling dient hiermee overweg te kunnen.
- De API-Management tooling bevat zelf functionaliteit waarmee firewalls geconfigureerd kunnen worden en past Cross-Origin Resource Sharing (CORS) toe om ongeoorloofd binnenkomend verkeer af te vangen.
- Tussen de API-Gateway en de gemeentelijke servicebus komt er maar 1 poort (tunnel) in de firewall. Deze wordt eenmalig aangelegd en kan voor allerlei soorten gegevensuitwisseling hergebruikt worden.
- De landelijke API-strategie (https://geonovum.github.io/KP-APIs/) omarmd wordt.



Figuur 2: Visualisatie 'schets van de technische architectuur'

3 Requirements

In dit hoofdstuk worden de requirements beschreven t.a.v. de functionaliteit van API-Management op verschillende aandachtsgebieden. In onderstaande visualisatie is de functionaliteit geplot op de referentiecomponenten.



Figuur 3: Functionaliteit binnen API-Management

3.1 API-Gateway

Flexibiliteit

- Messaging
  API-Management tooling geeft invulling aan het enterprise integration patern 'messaging', deze vorm van ontkoppeling is randvoorwaardelijk om silo's te kunnen elimineren.
- Inrichting van routering
  Het is mogelijk om (lightweight) routering te definiëren binnen de API-Management tooling. Routering kan ingericht worden op basis van verschillende criteria, zoals bijvoorbeeld afzender of inhoud.
- Geoptimaliseerd voor internetprotocollen
  In het landschap van gegevensuitwisseling worden de volgende uitwisselprotocollen toegepast: SOAP, JSON, GeoJSON, XML, WFS3.0. Ook een transformatie tussen de verschillende protocollen dient in voorkomende gevallen ondersteund te kunnen worden.
- Digikoppeling
  Naast de API-ondersteuning via SOAP/XML en REST/JSON wordt het Digikoppeling-protocol gehanteerd. De tooling voorziet hierin via de DAI-standaard (Digikoppeling Adapter Intern).
- Verbindingen mogelijk met authenticatie-voorzieningen zoals eIDAS, DigiD, eHerkenning en IRMA.
- NLX inways/outways
  Het heeft de voorkeur om makkelijk verbinding te kunnen leggen naar NLX (of een product dat uiteindelijk deze rol inneemt):
    - Om een API beschikbaar te stellen via NLX dient een zogenaamde inway aangelegd te worden. Deze inway is onderdeel van de NLX software en is via de API-Management tooling benaderbaar of te integreren.
    - Om een API die via NLX beschikbaar is aan consumers aan te bieden dient een zogenaamde outway aangelegd te worden. Deze outway is onderdeel van de NLX software en is via de API-Management tooling benaderbaar of te integreren.

Beveiliging

- Virtualiseren interne API’s
  Om voor de buitenwereld de interne URL's niet beschikbaar te stellen kunnen API's gevirtualiseerd worden. Hiermee dwing je externe partijen om via de juiste URL/poort binnen te komen en daarmee kan worden voldaan aan alle beveiligingsvoorschriften.
- Uitgifte API Keys (token service)
  Om er zeker ervan te zijn dat API's enkel worden aangeroepen door daarvoor bevoegde organisaties kan er gewerkt worden met API Keys. API Keys kunnen volstaan in testomgevingen of voor verbindingen t.a.v. open of niet-gevoelige data. In andere omgevingen wordt het gebruik van API Keys niet als voldoende ervaren, hiervoor wordt minimaal OAuth2.0 vereist.
- Authenticatie op basis van OAuth2.0 (iGOV-profiel)
  Interne consumers dienen zich te authentiseren voordat een API aangeroepen kan worden, er wordt in deze situatie gewerkt met refresh en access tokens.. Een koppelvlak tussen de API-Management tooling en de Identity Service Provider (ISP) van Drechtsteden is hierbij noodzakelijk. Drechtsteden zet als ISP de tool Active Directory in, met daar bovenop ADFS voor ondersteuning van Federation Services.
- Open ID connect (on top of OAuth2.0)
  Deze vorm van authenticatie werkt op basis van ID-tokens (JWT) en maakt het mogelijk om per gebruiker claims te definiëren waarin direct te herleiden is wat de

autorisatie van deze betreffende gebruiker is, waardoor voorkomen kan worden dat er technisch veel API's/resources[2] naast elkaar ondersteund moeten worden.

De API-Management tooling is in staat eenmalig (bij de eerste API-call van een consumer) de bijbehorende ID-token van de medewerker op te vragen bij de ISP. De API-Management tooling koppelt hieraan een access token en koppelt dit terug aan de consumer. Deze token is gekoppeld aan de combinatie applicatie/gebruiker en wordt vastgelegd in de API-Management tooling.
De consumer moet in staat zijn de access token (die dus gebruikerspecifiek is) mee te geven, zodat vervolg verzoeken niet door AD gecontroleerd hoeven worden. Hiervoor wordt OAuth2.0 toegepast.

De API-Management tooling heeft een verbinding met de ISP zodat gewijzigde autorisaties van een medewerker bekend zijn in de API-Management tooling.

- Er dient gewerkt te worden met een PKI-O certificaat voor JWT token encryptie. In de tokens zit dusdanig veel gevoelige informatie dat dit goed beveiligd moet worden. Daarom wordt ook voor de uitwisseling van de tokens encryptie toegepast. De ISP encrypt de tokens.

Robuustheid

- Load balancing
  In geval van piekbelasting is het mogelijk om dynamisch (binnen korte tijd) meer resources beschikbaar te stellen. Dit wordt technisch opgelost via technieken van virtualisatie/containerisation/sharding. Onder piekbelasting verstaat Drechtsteden een volume van 20x de norm.
- Rate limiting
  Bescherming tegen een bovenmatig aantal verzoeken die worden afgevuurd op de Drechtsteden-omgeving, waardoor er storingen op kunnen treden. Dit kan door DDoS-aanvallen namelijk het geval zijn, ook kan bij reguliere werking het 'spitsuur' zijn waardoor deze beveiliging ingeschakeld moet worden. Er kunnen verschillende profielen/plannen worden aangemaakt waarin deze quotas worden geconfigureerd. Een profiel/plan is te koppelen aan een specifieke API.
- Validatie
  Het valideren van inkomende en uitgaande API-calls tegen geldende definities. Ervoor zorgen dat de tooling is opgewassen tegen bedreigingen van buitenaf.
- Caching van de API-Gateway is instelbaar (tijd waarna de bron opnieuw bevraagd wordt).

3.2 API-Manager

Beveiliging

- Inrichten beveiligingsregels (policy)
  Voor iedere gegevensverbinding is het instelbaar welke maatregelen er genomen worden om de poort zo specifiek mogelijk open te zetten voor afnemers (het autoriseren van consumers (ook wel aangeduid als afnemers) en het inrichten van beveiligingscertificaten zijn daar voorbeelden van).
- Inlezen beveiligingscertificaten
  Beveiligingscertificaten worden ingezet op gegevensverbindingen tussen 2 applicaties, zodat de gegevens niet door een derde afgeluisterd kunnen worden (de certificaten zorgen voor versleuteling van de gegevensuitwisseling).
- Gegevensautorisatie
  Per profiel (overeenkomstig met een rol, raakvlak met RBAC) is het instelbaar welke data (op attribuutniveau) opgevraagd mag worden door een consumer van

[2] Een resource is een logische eenheid conform de RESTful principes (zie uitleg in landelijke API-strategie https://geonovum.github.io/KP-APIs/#restful-principes)

de API (consumer, in dit geval een applicatie i.c.m. de aanduiding van de gebruiker). Dit geeft mede invulling aan de eisen die gesteld worden vanuit wet- en regelgeving, namelijk autorisatie in te richten conform doelbinding. Het is gewenst om functionaliteit beschikbaar te hebben waarbij filtering op basis van autorisatie achteraf plaatsvindt (de API-management tooling haalt eerst de volledige set op bij de bron en filtert het antwoord voordat het naar de consumer teruggestuurd wordt).
Ook voor externe consumers geldt dat er een profiel gekoppeld kan worden dat de autorisatie bepaald. Dit geldt bijvoorbeeld voor klanten (burger/bedrijf) en ketenpartners.

Robuustheid

- Traffic Management
  Het toekennen van voorrang op de afhandeling van bepaalde calls is mogelijk, bijvoorbeeld door bulk-processen voor een korte periode voorrang te verlenen op andere calls. Hierdoor is gecontroleerd traffic management mogelijk, waardoor eventuele verstoringen op een later moment door piekbelasting juist kunnen worden voorkomen.

Realisatie API-serviceregistratie

De tooling ondersteunt de volgende functionaliteit:

- API-life cycle management
  Life cycle management is essentieel in een landschap dat continu verandert en een onzekere toekomst kent. Life cycle management omvat wat Drechtsteden betreft de volgende functionaliteit:
  - het creëren van API's
    door het importeren van externe configuraties/definities van API's of door het creëren van eigen API's. Eigen API's maken het mogelijk om Drechtsteden specifieke gegevensverbindingen op te zetten, als voorbeeld:
    - specifieke frontend API's te creëren op landelijke backend API's (voorbeeld 1 frontend API die 3 backend API's aanroept).
    - Drechtsteden specifieke bronnen te ontsluiten (zoals kernregistraties)
    - JSON API's te creëren boven op interne SOAP API's (transformatie).

    Het volgende kan worden vastgelegd per API:
    - Het definiëren van de URL waarmee de API aangeroepen kan worden door consumers.
    - Het definiëren van het endpoint (voor data ontsluiting of datamutaties).
    - Het inrichten van policies (zie beveiliging).
  - het testen van de API's (bijvoorbeeld op performance),
  - het aanbieden van nieuwe versies (eventueel via oplossingen zoals GIT)
  - het uitfaseren van oude versies.
- API creatie op Databases
  Gedurende de transitiefase richting een landschap dat is opgezet volgens de principes van Common Ground is het van meerwaarde om eenvoudig API's te creëren bovenop een (on-premise) database. Veel software leveranciers bieden namelijk, gedurende een transitiefase, nog geen API’s op databronnen. Data wordt eenvoudig ontsluitbaar, waar dat nu nog niet of slecht toegankelijk is. Dit geldt voor Oracle databases, als ook voor MySQL, Postgres en MongoDB. Drechtsteden wil dit technisch via REST Dataservices of JDBC op kunnen zetten. Op deze manier is het mogelijk eenvoudig:
  - Kolommen te exposen
  - Andere naamgeving toe te kennen aan attributen/tabellen
  - Datatypen op te geven
  - Generatie (en publicatie) van Open API docs
- Ontzorging consumers

Veel applicaties binnen Drechtsteden beschikken nog niet over alle functionaliteit om correct API's te kunnen aanbieden (providers) of aanroepen (consumers). Dit komt o.a. doordat leveranciers zich al die tijd vastgehouden hebben aan StUF. Door ondersteuning te bieden aan deze applicaties (via StUF-API transformaties of API's aan te bieden op datasets) kan de transitie naar brede inzet van API's toch al in gang gezet worden (zie ook 3.1 flexibiliteit).

- Import/Export tussen gemeenten
  Gemeenten kunnen grote efficiency voordelen behalen door de API-serviceregistratie met elkaar uit te wisselen via Open API Specificatie versie 3.0 (OAS3.0). Het is mogelijk om (delen van) de API-serviceregistratie van Drechtsteden te exporteren, zodat andere gemeenten die ook kunnen gebruiken. Daarnaast is het mogelijk zijn (delen van) de configuratie van andere gemeenten te importeren.

Monitoring & Analysis

- API use dashboards/Analytics
  Voor Beheerders en Management interessant inzicht in welke API's wanneer en hoe vaak gebruikt worden en wat de performance is. Op basis van deze informatie kan bijvoorbeeld gesleuteld worden aan de inrichting om het landschap efficiënter in te richten.
- Logging
  De logging van het gebruik van de API's is noodzakelijk voor auditing doeleinden (i.h.k.v. privacy, beveiliging en transparantie). Het achteraf kunnen inzien:
  - Wie heeft data geraadpleegd?
  - Welke data is geraadpleegd?
  - Waarom de data is geraadpleegd?
  - Wanneer de data is geraadpleegd
  - Hoe de data is geraadpleegd?

  De logging over het afgelopen jaar is op een efficiënte wijze raadpleegbaar/doorzoekbaar, bijvoorbeeld via Dashboards en/of via de zoekingang BSN om op die manier makkelijk te achterhalen op welke momenten bepaalde persoonsgegevens zijn geraadpleegd door wie en waarom. Het is aanbevolen dat generieke logging kan worden uitgewisseld met de tool Zabbix. De tool die momenteel door Drechtsteden centraal wordt ingezet.
- Export data for audits
  Voor audit-doeleinden exporteren van logging (naar CSV-formaat of andere gangbare standaarden).
- API billing (Monetizing)
  Va rapportages/dashboards inzicht in het gebruik van de API's waardoor het mogelijk is om het gebruik van API's door te belasten aan de consumer. Dit is voor Drechtsteden interessant om kosten eventueel door te belasten op de afzonderlijke organisaties/gemeenten binnen de Drechtsteden.
- Alerts
  Het versturen van (SMS en/of mail) notificaties aan bijvoorbeeld beheerders indien bepaalde gebeurtenissen optreden (bijvoorbeeld wanneer een bepaalde gegevensverbinding uit de lucht is of certificaten op korte termijn zullen verlopen).

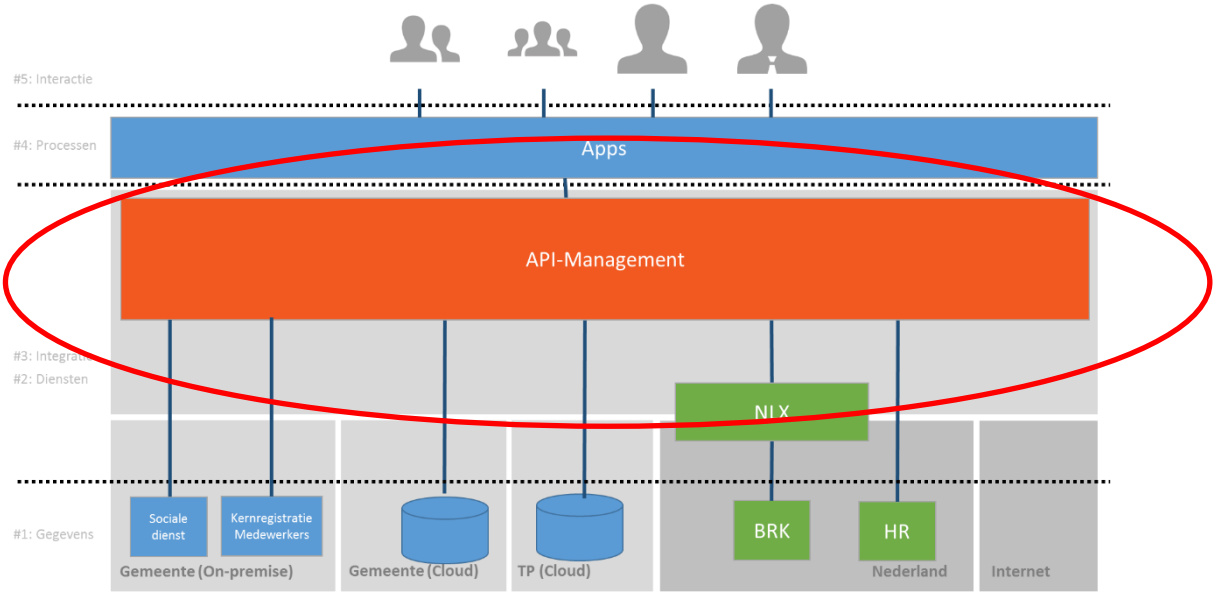
3.3 API-Portaal

- Serviceregistratie (ook wel aangeduid als API-Explorer of API-Gallery)
  Voor medewerkers betrokken bij de software ontwikkeling is het interessant te weten welke API's beschikbaar zijn, welke data (of functionaliteit) ermee opgehaald kan worden en hoe de API aangeroepen moet worden (zie ook API docs).

- De serviceregistratie is eenvoudig doorzoekbaar. Daarnaast is een Swagger-plugin gewenst, zodat API-definities op basis van de Open API Specificatie versie 3.0 (OAS3.0) makkelijk overgenomen kunnen worden van andere (externe) bronnen.
- API Docs
  Alle documentatie gerelateerd aan de API zijn via het portaal eenvoudig te beheren en terug te vinden.
- Voor niet openbare API's geldt dat een kandidaat consumer via het portaal een verzoek kan inschieten tot het mogen gebruiken van de API. Dit verzoek komt bij de beheerders te liggen ter afhandeling.
- Forums
  Het heeft de voorkeur van Drechtsteden dat de tooling het mogelijk maakt dat ontwikkelaars eenvoudig met elkaar in contact treden t.a.v. de realisatie van de API's. Dit kan eventueel via een forum.
- Share Sample code
  Ontwikkelaars die software maken die een API-call kunnen versturen zijn gebaat bij het verkrijgen van voorbeeldcode. Hierdoor wordt de ontwikkeltijd aan consumer-zijde nog verder teruggebracht.

4 Beheer

De beheerwerkzaamheden voor de API-Management tooling worden uitgevoerd door zowel Drechtsteden als door de leverancier (zie de afbakening in onderstaande visualisatie).



Figuur 4: Afbakening API-Management

Globaal kan gesteld worden dat voor beheer van API-Management Drechtsteden als opdrachtgever functioneel bepaalt wat er moet gebeuren en daarmee de regierol vervult en de leverancier verantwoordelijk is voor de daadwerkelijke uitvoering van het beheer.

Concreet betekent dit dat de onderstaande beheerwerkzaamheden onder de verantwoordelijkheid van respectievelijk Drechtsteden en leverancier vallen (zie tabellen op de volgende pagina's).

Onderdeel	Drechtsteden
Keten-regie aansluiting afnemers	Afstemming met afnemers Drechtsteden en daarmee de specificaties van de gegevensverbindingen helder krijgen (definitie in gegevensleveringsovereenkomst, GLO) - Doelbinding - Autorisatie - Gegevensset - Verantwoordelijke organisatie(onderdelen) - Informatiebeveiliging
	Verzoek honoreren, in samenwerking met Juridische zaken en architecten.
	Geplande wijzigingen doorspreken die impact hebben op afnemers.
	Planningsafspraken maken met afnemers en leverancier over daadwerkelijke aansluitingsmomenten
Uitvoeren aansluiting afnemers	- Ad hoc informatieverzoeken van afnemers faciliteren (API's die niet standaard worden geleverd door de leverancier).
Keten-regie aansluiting bronhouders	Afstemming met bronhouders en beheerders van betreffende bronsystemen binnen Drechtsteden. Specificaties gegevensverbindingen helder krijgen (definitie in GLO) - Doelbinding - Autorisatie - Gegevensset - Verantwoordelijke organisatie(onderdelen) - informatiebeveiliging
	Nieuwe gegevensverbindingen voor nieuwe lokale databronnen specificeren - Op basis van geldend informatiemodel dat de databron beschrijft. - Views/Datamarts op tabellen creëren (eventueel raakvlak met gemeentelijke servicebus en ETL-jobs). - Aanleveren specificaties datamodel van de bron voor API's die direct een database benaderen. - Specificaties opstellen (op basis van OpenAPI v3.0 in YAML 2.0 formaat) van te realiseren API's
	Gewijzigde gegevensverbindingen voor gewijzigde lokale databronnen specificeren - Op basis van wijzigingen vanuit software leverancier die de software levert waarin de brondata zich bevindt. - Views/Datamarts op tabellen aanpassen (eventuele aanpassingen in gemeentelijke servicebus en ETL-jobs). - Aanleveren gewijzigde specificaties datamodel van de bron voor API's die direct een database benaderen. - Specificaties aanleveren (op basis van minimaal OpenAPI v3.0 in YAML 2.0 formaat) voor nieuwe versie van API's.
	Planningsafspraken maken met bronhouders (en beheerders betreffende bronsystemen binnen Drechtsteden) en leverancier over daadwerkelijke aansluitingsmomenten op nieuwe en gewijzigde gegevensverbindingen.
Firewall/ certificaten	- Regie over de verschillende beheerpartijen (Beheer Drechtsteden, Beheerpartij Drechtsteden-Cloud en Beheerpartij leverancier API-Management). - Firewall beheer (toegang tot Drechtsteden-on premise en Drechtsteden Cloud[3]).
	Aanvragen/verlenging PKI-O
	Aanlevering PKIO-certificaten aan Leverancier

[3] Niet te verwarren met een leverancier specifieke Cloud. Daarvoor doen die leveranciers namelijk specifiek zelf het Firewall beheer.

Database toegang	Database beheer (toegang Leverancier tot Database voor API's die direct de bron-database benaderen; hetzij Drechtsteden OnPremise, hetzij Drechtsteden Cloud).
Authenticatie	Volledig beheer op de Active Directory van Drechtsteden.

Onderdeel	Leverancier
Applicatie-beheer	- Updates Major releases uitvoeren.
Uitvoeren aansluiting afnemers	- Nieuwe gegevensverbindingen inrichten - API-tokens uitgeven - API-tokens toekennen aan afnemer (connect met AD) - Beveiligingscertificaten/endpoints inrichten - Inrichting gegevensautorisatie (conform GLO)
Beschikbaar stellen API's	Lifecycle management API's conform landelijke API strategie Overheid, waaronder: - Het creëren van API's - Het testen van de API's (bijvoorbeeld op performance) - Het aanbieden van nieuwe versies - Het uitfaseren van oude versies - Serviceregistratie (API-catalog) vullen Lokale bronnen (binnen Drechtsteden): - Wordt uitgevoerd op basis van de specificaties en verzoeken van Drechtsteden Bronnen Third parties (ketenpartijen waar Drechtsteden geen invloed op kan uitoefenen): - Monitoring nieuwe versie API - Nieuwe versie API beschikbaar stellen - Tijdig informeren Drechtsteden dat er een nieuwe versie ondersteund gaat worden. Bronnen inschrijver (bronnen die de software leverancier van API-Management zelf aanbiedt): - Monitoring nieuwe versie API - Nieuwe versie API beschikbaar stellen - Tijdig informeren Drechtsteden dat er een nieuwe versie ondersteund gaat worden. Landelijke bronnen: - Monitoring nieuwe versie landelijke API - Nieuwe versie landelijke API beschikbaar stellen - Tijdig informeren Drechtsteden dat er een nieuwe versie ondersteund gaat worden.
Beheer Gegevens-verbindingen	- Monitoring actieve gegevensverbindingen - Weblog bekijken bij incidenten - Verstoringen oplossen - Beheer connecties bij wijzigingen beveiligingscertificaten/endpoints
Firewall/ certificaten	- Firewall beheer (Cloud-2-Cloud) - Beveiligingscertificaten uitgeven - Beveiligingscertificaten inrichten - Monitoring op het verlopen van certificaten - Certificaten vernieuwen - Periodieke update owasp webfirewall rules
Server beheer	- Beheeractiviteiten: Monitoren of services draaien (op platformniveau) - Proactief capacity management (cpu, memory, disk resources)

	- Weblog bekijken bij incidenten - Verstoringen oplossen - Uitwijkmogelijkheden bieden