

Sprint 6: Techniek

Autorisatie & hot potatoes



Onderwerpen

- Autorisatie
- Componentaanpassingen (RGBZ)
- Documentatie
- Praktisch (Amsterdam)

Autorisatie

Hoofdthema van deze sprint

User stories

Filters ▾ Labels Milestones New issue

Clear current search query, filters, and sorts

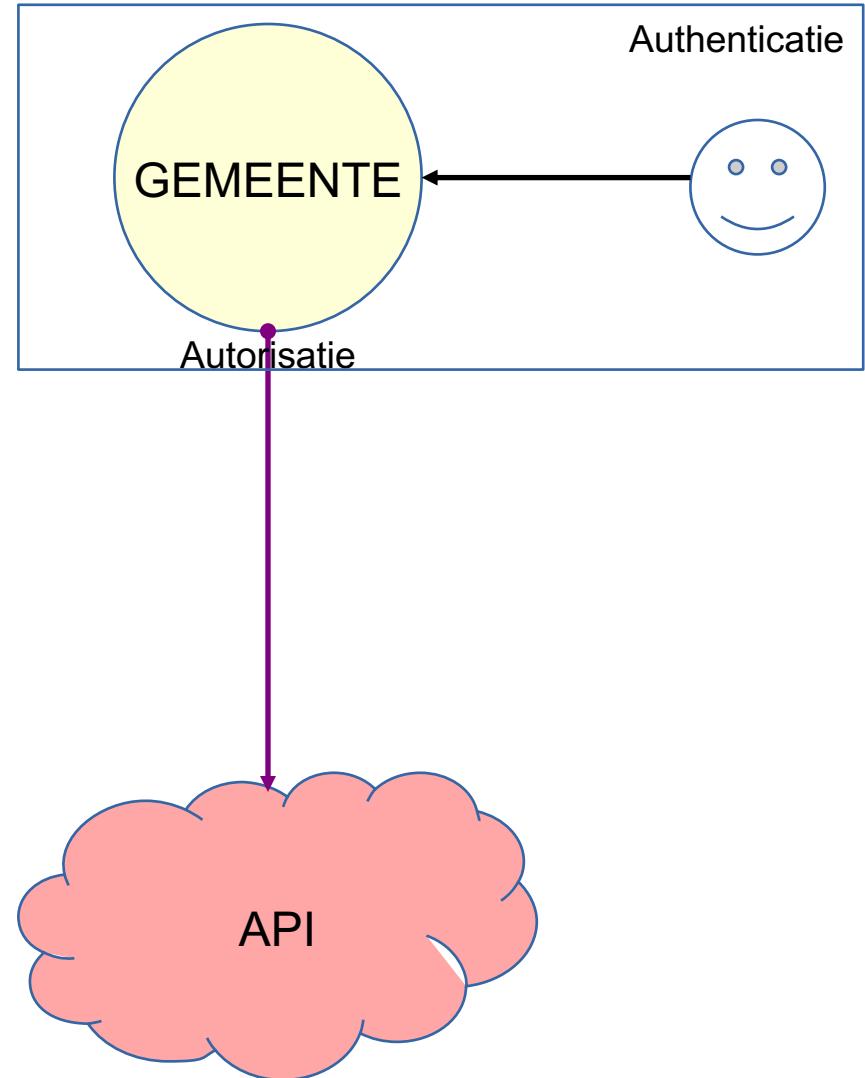
3 Open ✓ 1 Closed Author ▾ Labels ▾ Projects ▾ Milestones ▾ Assignee ▾ Sort ▾

Issue	Author	Labels	Milestones	Comments
<input type="checkbox"/> Feature/scopes ✓ Review Pull-request autorisatie #525 by sergei-maertens was merged 3 hours ago • Approved 3 of 4 Sprint 6		6		
<input type="checkbox"/> Als api-ontwikkelaar wil ik een standaardmechanisme om scopes te kennen van een app Prio H autorisatie #428 opened on Oct 1 by sergei-maertens 22 of 22 Sprint 6		3		
<input type="checkbox"/> Als projectlid wil ik dat de referentieimplementaties de implementeerbaarheid van de scopes aantonen Prio H autorisatie blok #425 opened on Oct 1 by sergei-maertens 8 of 24 Sprint 6		2		
<input type="checkbox"/> Als projectlid wil ik weten welke scopes voor autorisatie we onderkennen in de API Overleg nodig Prio H autorisatie #424 opened on Oct 1 by sergei-maertens 8 of 20 Sprint 6		10		

Inleiding en definities

Wat is autorisatie?

- Authenticatie: wie ben je?
- Autorisatie: wat mag je?



Autorisatie: verifieerbare claims

Claims worden gebruikt om operaties/gegevens toe te staan

- scopes: is een operatie wel/niet toegelaten (zaak_create, status_create)
- zaaktypes: limiteert zaken/statussen... tot deze zaaktypes
- Later waarschijnlijk: vertrouwelijkheidsaanduiding

zaak_create

Maak een ZAAK aan.

Indien geen identificatie gegeven is, dan wordt deze automatisch gegenereerd.

De URL naar het zaaktype wordt gevalideerd op geldigheid.

AUTHORIZATIONS:

JWT-Claims (`zds.scopes.zaken.aanmaken`)

```
{  
  "zds": {  
    "scopes": [  
      "zds.scopes.zaken.aanmaken"  
    ],  
    "zaaktypes": [  
      "https://haarlem.ztc.nl/api/v1/zaaktypen/123",  
      "https://haarlem.ztc.nl/api/v1/zaaktypen/124",  
    ]  
  }  
}
```

Autorisatie: transport & claim-verificatie?

JSON Web Token (JWT) crash course

- Header: type + algoritme (+ custom keys)
- Payload: registered claims (iss, exp, sub, aud...) + public claims + **private claims**
- Signature: cryptografisch secure ondertekening dat er niet gesjoemeld is met de payload

- Locatie: Gaat in de HTTP Authorization header



Voorbeeld

Encoded

PASTE A TOKEN HERE

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsImNs  
aWVudF9pZGVudGlmaWVyIjoiZHVtblXkteXMxazJG  
ZUZ6azdKIn0.eyJpc3MiOiJkdW1teS15czFrMkZl  
RnprN0oiLCJpYXQiOjE1NDI4MTQzMzMsInpkcyI6  
eyJzY29wZXMiOlsiemRzLnNjb3Blcy56YWtlbi5s  
ZXplbiJdLCJ6YWFrh1lwZXMiOlziaHR0cHM6Ly9y  
ZWYudHN0LnZuZy5jbG91ZC96dGMvYXBpL3YxL2Nh  
dGFsb2d1c3N1bi9mN2FmZDE1Ni1j0GY1LTQ2NjYt  
YjhINS0y0GE0YTliNWRmYzcuemFha3R5cGVuLzAx  
MTlkZDR1LTdiZTktNDc3ZS1iY2NmLTc1MDIzYjE0  
NTNjMSJdfX0.fkB08y2yZchJmFIgJ_Fkw9mOhXN  
vjVh0overfuo9GA
```

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{  
  "typ": "JWT",  
  "alg": "HS256",  
  "client_identifier": "dummy-ys1k2FeFzk7J"  
}
```

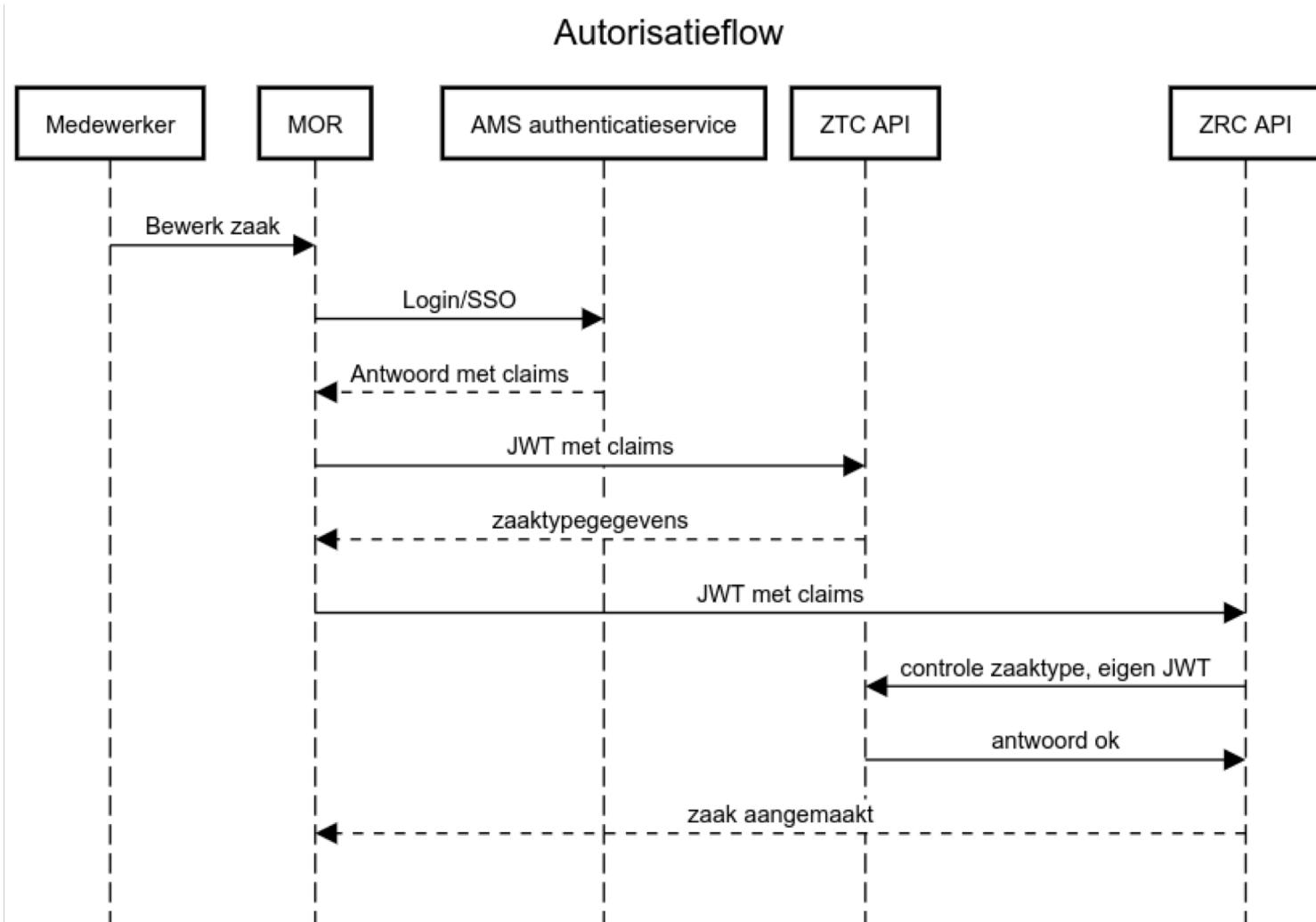
PAYOUT: DATA

```
{  
  "iss": "dummy-ys1k2FeFzk7J",  
  "iat": 1542814133,  
  "zds": {  
    "scopes": [  
      "zds.scopes.zaken.lezen"  
    ],  
    "zaaktypes": [  
  
      "https://ref.tst.vng.cloud/ztc/api/v1/catalogussen/f7af15  
6-c8f5-4666-b8b5-28a4a9b5dfc7/zaaktypen/0119dd4e-7be9-  
477e-bccf-75023b1453c1"  
    ]  
  }  
}
```

VERIFY SIGNATURE

```
HMACSHA256(  
  base64UrlEncode(header) + "." +  
  base64UrlEncode(payload),  
  Cm57k9b0olamo8dh2DwG  
)  secret base64 encoded
```

Sequence diagram flow

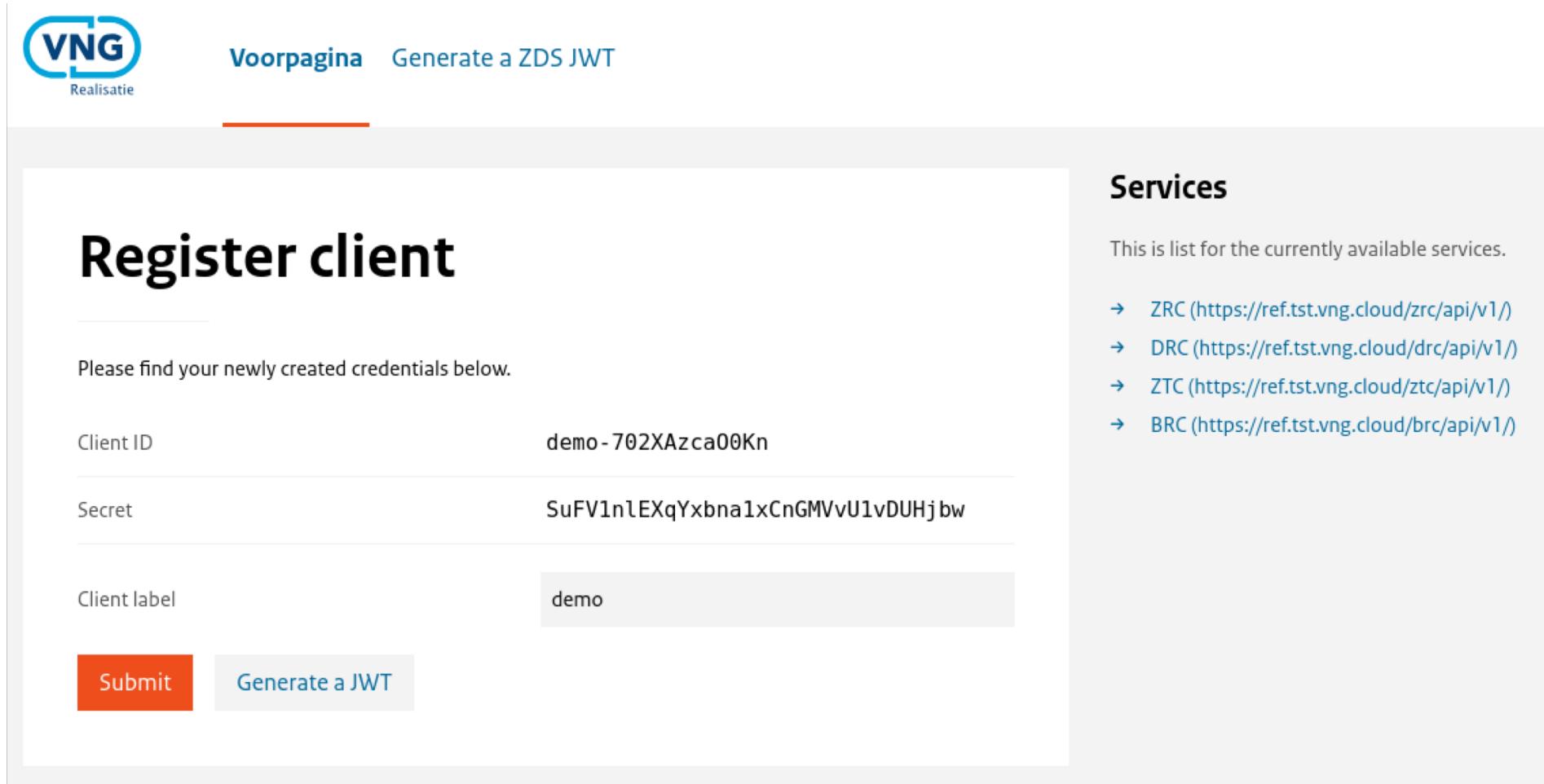


Tool: token-issuer

Gemeentes hebben hun authenticatie in eigen beheer

- Generatie client ID & Secret
- Registratie client ID & Secret bij services
- Genereer JWT met client ID & Secret

<https://ref.tst.vng.cloud/tokens/>



The screenshot shows a web application interface for generating ZDS JWT tokens. At the top, there's a header with the VNG Realisatie logo and a navigation bar with 'Voorpagina' and 'Generate a ZDS JWT'. The main content area has a title 'Register client' and a message 'Please find your newly created credentials below.' Below this, there are three input fields: 'Client ID' (demo-702XAzca00Kn), 'Secret' (SuFV1n1EXqYxbna1xCnGMVvU1vDUHj bw), and 'Client label' (demo). At the bottom are two buttons: 'Submit' (orange) and 'Generate a JWT' (grey). To the right, a sidebar titled 'Services' lists available endpoints: ZRC, DRC, ZTC, and BRC, each with its corresponding URL.

Voorpagina Generate a ZDS JWT

Register client

Please find your newly created credentials below.

Client ID	demo-702XAzca00Kn
Secret	SuFV1n1EXqYxbna1xCnGMVvU1vDUHj bw
Client label	demo

Submit **Generate a JWT**

Services

This is list for the currently available services.

- ZRC (<https://ref.tst.vng.cloud/zrc/api/v1/>)
- DRC (<https://ref.tst.vng.cloud/drc/api/v1/>)
- ZTC (<https://ref.tst.vng.cloud/ztc/api/v1/>)
- BRC (<https://ref.tst.vng.cloud/brc/api/v1/>)

<https://ref.tst.vng.cloud/tokens/generate-jwt/>

Generate a ZDS JWT

Componentaanpassingen

RGBZ-wijzigingen en wijzingen wegens RGBZ

Besluitenregistratie (BRС)

- Besluit.datum: van datetime naar datum → geen vals gevoel van precisie
- Besluit.toelichting: geen karakterlimiet (RGBZ aanpassing)
- Besluit.identificatie en Besluit.verantwoorelijkeOrganisatie mogen niet gewijzigd worden
- Besluit.vervalreden: systeemcodes toegevoegd + weergave veld

vervalreden	string (Vervalreden) Enum: "tijdelijk" "ingetrokken_overheid" "ingetrokken_belanghebbende" De omschrijving die aangeeft op grond waarvan het besluit is of komt te vervallen. De mapping van waarden naar weergave is als volgt:
	<ul style="list-style-type: none">• <code>tijdelijk</code> - Besluit met tijdelijke werking• <code>ingetrokken_overheid</code> - Besluit ingetrokken door overheid• <code>ingetrokken_belanghebbende</code> - Besluit ingetrokken o.v.v. belanghebbende
vervalredenWeergave	string (Vervalreden weergave) non-empty

Zakenregistratie (ZRC)

- Zaak.einddatum: blijft datum – ook hier vals gevoel van precisie vermijden
- Meer velden zoals identificatie niet-wijzigbaar gemaakt

Documentenregistratie (DRC)

- Kritiek: in de ObjectInformatieObject resource is informatie verdwenen uit het informatiemodel: aardRelatie
- Ontwikkelaar gebruikt API-spec en hoeft niet RGBZ te kennen
- aardRelatie toegevoegd, wat volgt uit het objectType
- Eisen aan de server/systeem-kant!

De registratiedatum wordt door het systeem op 'NU' gezet. De aard_relatie wordt ook door het systeem gezet.

Bij het aanmaken wordt ook in de bron van het OBJECT de gespiegelde relatie aangemaakt, echter zonder de relatie-informatie.

Titel, beschrijving en registratiedatum zijn enkel relevant als het om een object van het type ZAAK gaat (aard relatie "hoort bij").

AUTHORIZATIONS:

JWT-Claims

REQUEST BODY SCHEMA: application/json

informatieobject <small>required</small>	string <uri> (Informatieobject)
object <small>required</small>	string <uri> (Object) <small>[1 .. 200] characters</small> URL naar het gerelateerde OBJECT.
objectType <small>required</small>	string (Objecttype) Enum: <small>"besluit" "zaak"</small>
titel	string (Titel) <small><= 200 characters</small> De naam waaronder het INFORMATIEOBJECT binnen het OBJECT bekend is.
beschrijving	string (Beschrijving) Een op het object gerichte beschrijving van de inhoud van het INFORMATIEOBJECT.

Documentatie

Herstructureren en herdesign

<https://ref.tst.vng.cloud/>

Praktisch

Aanpassingen naar aanleiding van *echt* gebruik

Amsterdam: opvragen statussen van een zaak

Fixes #518 -- added status filter on zaak & statustype
#524

Merged

sergei-maertens merged 1 commit into master from feature/us-518-filter-status 20 days ago

Cross-Origin Resource Sharing (CORS) toegevoegd

ZRC API geeft foutmelding in REDOC #450

 **Closed** michielverhoef opened this issue on Oct 9 · 4 comments

Stand van zaken

Sprintinventaris

4 Sprint 6 - demo .. november 2018 + ...

Api-Version header ontbreekt in API spec en referentie-implementatie(s)

#563 opened by sergei-maertens

bug

Location header ontbreekt in OAS spec ...

#562 opened by sergei-maertens

bug

Als architect wil ik een heldere architectuuruitwerking voor de straatartiest

#352 opened by jgortmaker1

impediment

Als gebruiker van de referentieimplementaties wil ik een voorbeeld van een rol-naar-scope mapper

8 of 21

#427 opened by sergei-maertens

Prio H autorisatie

15 In progress + ...

15 In progress + ...

Als API-lab deelnemer wil ik tutorials kunnen volgen om snel de referentie implementaties werkend te krijgen

1 of 3

#545 opened by joeribekker

API-lab

Als developer wil ik dat niet toegestane query-params een error geven

8 of 17

#420 opened by joeribekker

Developer algemeen Improvement

Prio H

Notificeren over zaken

#397 opened by jgortmaker1

Overleg nodig Prio H architectuur

Relatie proces - zaak

#392 opened by jgortmaker1

Overleg nodig architectuur

Hoe leggen we relatie tussen zaak en objecten?

0 of 2

#394 opened by jgortmaker1

architectuur

Demo sprint 6 22 november 2018 in Rotterdam

2 of 18

#515 opened by TCIMEddy

5 Review + ...

5 Review + ...

Functionele documentatie 'zaken' API

#476 opened by michielverhoef

Documentatie

Changes requested

Functionele documentatie 'informatieobjecten' API

#457 opened by michielverhoef

Documentatie

Changes requested

Als projectlid wil ik functionele documentatie per API

2 of 5

#188 opened by michielverhoef

Functionele docum... Prio H WIP meta

Functionele documentatie 'zaaktypen' API

#451 opened by michielverhoef

Documentatie

Changes requested

Als burger wil ik de status en de relevante documenten van mijn inzage verzoek kunnen inzien op de PIP van de gemeente Delft

14 of 17

#154 opened by RitaBerghuis

AVG Prio H

21 Done - Sprint 6 + ...

21 Done - Sprint 6 + ...

Feature/scopes

#525 opened by sergei-maertens

Review Pull-request autorisatie



Changes approved

:construction_worker: Fixing CI/CD pipeline

#561 opened by sergei-maertens

ops

Changes approved

Ref. #162 -- toevoeging BRC

#362 opened by sergei-maertens

Prio H Review Pull-request



Changes approved

Welke bakjes onderkennen we?

#395 opened by jgortmaker1

architectuur



Feature/#1 jekyll

#548 opened by svenvandescheur

Documentatie

Changes approved

Switch documentatietooling (van Hugo naar Jekyll)

#414 opened by JoseJBoon

Automated as Done



Automated as To do

Manage

Manage

Manage

