Instructie aansluiten Terugmelding bronhouder API

De Terugmelding bronhouder API is beveiligd middels de OAuth 2.0 specificatie. Dit document biedt een instructie voor het aansluiten op die API.

Change log

- 1.0 02-12-2021: Eerste versie
- 1.1 06-12-2021: Versie na review
- 1.2 16-12-2021: Feedback verwerkt bij stap 2 (geen client_secret)
- 1.3 14-09-2022: Tekst verbeterd
- 1.4 17-04-2023: PKCE flow toegevoegd
- 1.5 03-05-2023: Geldigheid authorization token aangepast en tekst verbeterd
- 2.0 01-07-2024: Nieuwe Terugmelding Bronhouder API versie 2.0

Inhoud

Werking

Bij elk request naar het API endpoint moet een access token in de header van het request meegestuurd worden. Om dit token te verkrijgen, moeten onderstaande stappen doorlopen worden.

1. Client applicatie aanmelden. Dit moet éénmalig per client applicatie gedaan worden.
2. Authorization token opvragen. Dit moet éénmalig per sessie gedaan worden.

   NB Bij voorkeur wordt hierbij gemaakt van Proof Key for Code Exchange (PKCE) flow.

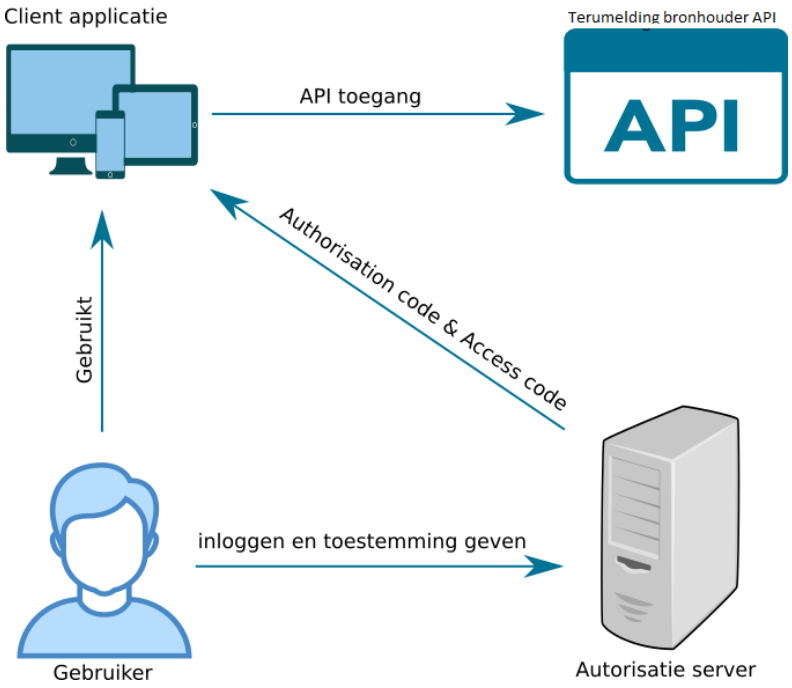
3. Access token opvragen. Dit token geeft toegang tot de API. Dit token is één uur geldig en zal daarna ververst moeten worden.
4. Access token gebruiken.
5. Access token verversen. Als het access token verlopen is, kan deze ververst worden. Daarvoor hoeven stap 1 t/m 3 niet opnieuw doorlopen te worden.

Let wel: in deze handleiding wordt uitgegaan van de *productie* omgeving bij de authorization URL, de token URL en het API endpoint. Voor de acceptatie omgeving is dit respectievelijk:

https://authorization.acceptatie.kadaster.nl/auth/oauth/v2/authorize?response_type=code&client_id=[client_id]&redirect_uri=[redirect_uri]&scope=[scope]&code_challenge=[code_challenge]&code_challenge_method=S256

https://authorization.acceptatie.kadaster.nl/auth/oauth/v2/token

https://service10.acceptatie.kadaster.nl/tms/bronhouders/v2/terugmeldingen



1. Client applicatie aanmelden

Voordat u kunt beginnen met testen van uw client applicatie, dient u deze aan te melden bij het Kadaster. U dient hierbij uw callback/redirect url op te geven. Dit kan via een formulier op de Kadaster website. Dit formulier vindt u op:
https://formulieren.kadaster.nl/terugmelding-bronhouder-api-oauth

Na goedkeuring van de aanvraag krijgt u een client_id en client_secret.

Er is een acceptatie omgeving beschikbaar voor test doeleinden en een productie omgeving.

Scopes

Voor de Terugmelding bronhouder API kennen we de volgende scopes:

Scope	**Omschrijving**
tms.bgt.readonly	Kunnen lezen van eigen terugmeldingen van de BGT.
tms.bgt	Kunnen wijzigen van eigen terugmeldingen van de BGT + indienen van nieuwe terugmeldingen op alle registraties.
tms.bag.readonly	Kunnen lezen van eigen terugmeldingen van de BAG.

tms.bag	Kunnen wijzigen van eigen terugmeldingen van de BAG + indienen van nieuwe terugmeldingen op alle registraties.

2. Authorization token opvragen

Rechten voor gebruik van het API endpoint zijn gekoppeld aan Mijn Kadaster accounts. De gebruiker zal de client applicatie hiervoor per sessie toestemming moeten geven door in te loggen.

Proof Key for Code Exchange (PKCE) flow

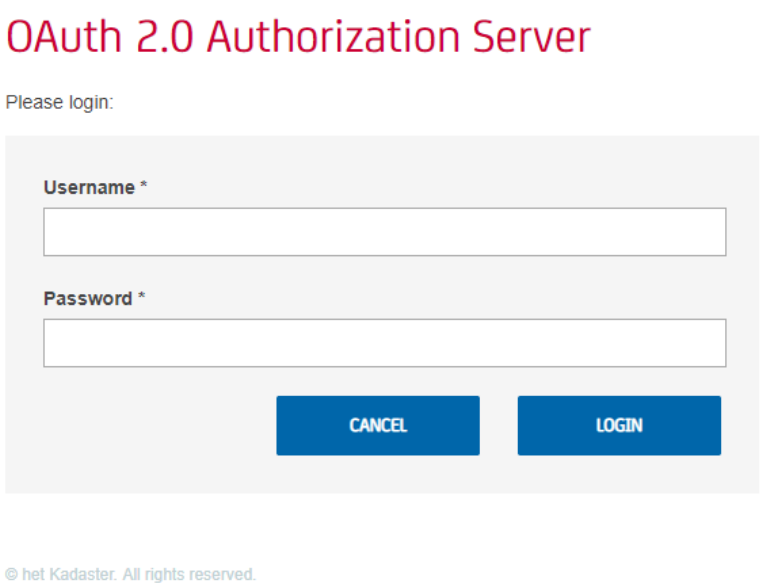
Bij voorkeur wordt er gebruik gemaakt van de PKCE flow waarmee voor extra beveiliging wordt gezorgd in het verkeer tussen de client applicatie en de authorization server. Hiermee kan de authorization server het authorization request koppelen aan het token request en controleren of het afkomstig is van dezelfde client applicatie (en de code dus niet is onderschept en geïnjecteerd is in een andere sessie). De client applicatie moet hiervoor een **code_verifier** genereren en een hier op gebaseerde **code_challenge** die is gemaakt op basis van een **code_challenge_method** (alleen “S256” mogelijk)**.** De **code_challenge** en **code_challenge_method** moeten worden meegestuurd tijdens het opvragen van het authorization token. Later bij het opvragen van het access token wordt de **code_verifier** meegestuurd om te bewijzen dat het request van dezelfde client applicatie afkomstig is. Zie voor meer informatie over PKCE en de implementatie hiervan: https://oauth.net/2/pkce/ en https://auth0.com/docs/get-started/authentication-and-authorization-flow/authorization-code-flow-with-proof-key-for-code-exchange-pkce

De call naar de authorization URL komt er dan als volgt uit te zien:

https://authorization.kadaster.nl/auth/oauth/v2/authorize?response_type=code&client_id=[client_id]&redirect_uri=[redirect_uri]&scope=[scope]&code_challenge=[code_challenge]&code_challenge_method=S256

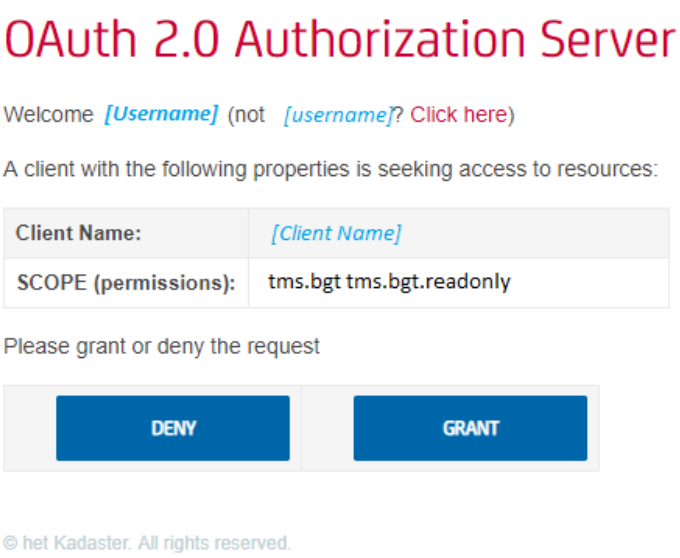
NB Bij meerdere scopes scheiden van elkaar met “+”.

Optioneel is het mogelijk om *geen* gebruik te maken van de PKCE flow. Daarmee wordt de call naar de authorization URL als volgt:
https://authorization.kadaster.nl/auth/oauth/v2/authorize?response_type=code&client_id=[client_id]&redirect_uri=[redirect_uri]&scope=[scope]



Indien eHerkenning actief is voor uw client applicatie, zal er eerst een keuze scherm te zien zijn:

Na het inloggen met een Mijn Kadaster account of via eHerkenning verschijnt onderstaand scherm:



Klik op GRANT als de gegevens kloppen.

Controleer of de Client Name overeen komt met uw aangemelde client applicatie.

De gebruiker wordt daarna doorgestuurd naar de opgegeven callback/redirect url. Uit de request parameters kan het authorization token gehaald worden. Bijvoorbeeld:

http://localhost:14057/authorize/?code=42283687-7c09-4018-8a7a-9e9533366dbb.

Dit authorization token is 300 seconden geldig, vraag daarom spoedig daarna een access token op.

3. Access token opvragen

Met het client_id, client_secret en dit authorization token kunnen we een access token opvragen via de token URL.

request (POST)

Token URL: https://authorization.kadaster.nl/auth/oauth/v2/token

Header: geef in de header als ContentType application/x-www-form-urlencoded mee.

Body: de parameters moeten in de body meegegeven worden. Zie voorbeeld:

client_id=[client_id]&client_secret=[client_secret]&grant_type=authorization_code&code=[authorisation_token]&redirect_uri=[redirect_url]&code_verifier=[code_verifier]

Proof Key for Code Exchange (PKCE) flow

Indien er eerder is gekozen om gebruik te maken van de PKCE flow wordt er bij het opvragen van het access token de **code_verifier** meegestuurd vanuit de client applicatie. Hiermee geeft de client applicatie bewijs dat dit request afkomstig is van dezelfde client applicatie als degene die het request heeft gedaan voor het authorization token.

Als er voor is gekozen om *geen* gebruik te maken van de PKCE flow, komt de body er als volgt uit te zien:

client_id=[client_id]&client_secret=[client_secret]&grant_type=authorization_code&code=[authorisation_token]&redirect_uri=[redirect_url]

In beide situaties is de response hetzelfde.

response

{

"access_token": "9e25ab45-82a4-4f9e-8bf6-b9ef0eb7568e",
"token_type": "Bearer",
"expires_in": 3600,
"refresh_token": "a413b322-59ab-4573-dd0b-000547d929b3",
"scope": "tms.bgt"

}

Dit access token en refresh token moet door de client applicatie op een veilige manier bewaard worden bijvoorbeeld via cookies. Het access token moet meegestuurd worden bij elke call naar de Terugmelding bronhouder API.

4. Access token gebruiken

Een voorbeeld van een API call naar het API endpoint met access token via curl.

curl

--header 'Authorization: Bearer 9e25ab45-82a4-4f9e-8bf6-b9ef0eb7568e'

Ophalen van nieuwe terugmeldingen:

GET: https://service10.kadaster.nl/tms/bronhouders/v2/terugmeldingen?statusCode=NIEUW

Wijzigen van een terugmelding:

PATCH: https://service10.kadaster.nl/tms/bronhouders/v2/terugmeldingen/3587

5. Access token verversen

Het access token is 1 uur geldig. Als het access token verlopen is, dan kan een nieuw access token en refresh token opgevraagd worden.

request (POST)

URL: https://authorization.kadaster.nl/auth/oauth/v2/token

Header: Geef in de header als ContentType application/x-www-form-urlencoded mee.

Body: De parameters moeten in de body meegegeven worden. Zie voorbeeld:

client_id=[client_id]&client_secret=[client_secret]&grant_type=refresh_token&refresh_token=[refresh_token]

response

{

```
  "access_token": "eb7929c4-4259-442c-931f-14fba228a6aa",
  "token_type": "Bearer",
  "expires_in": 3600,
  "refresh_token": "29786b93-24ca-4e91-9c8c-b87715f48ba9",
  "scope": "tms.bgt"
}
```