Welkom

We starten 9.15 uur

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Ketendemo 24 november 2022 hybride –sessie

Voor de deelnemers online:

Zet jouw microfoon op ‘mute’

Voor een rustig beeld vragen we je om de camera zelf uit te schakelen

Wij maken opnames van deze sessie

Steek de hand op voor het stellen van vragen

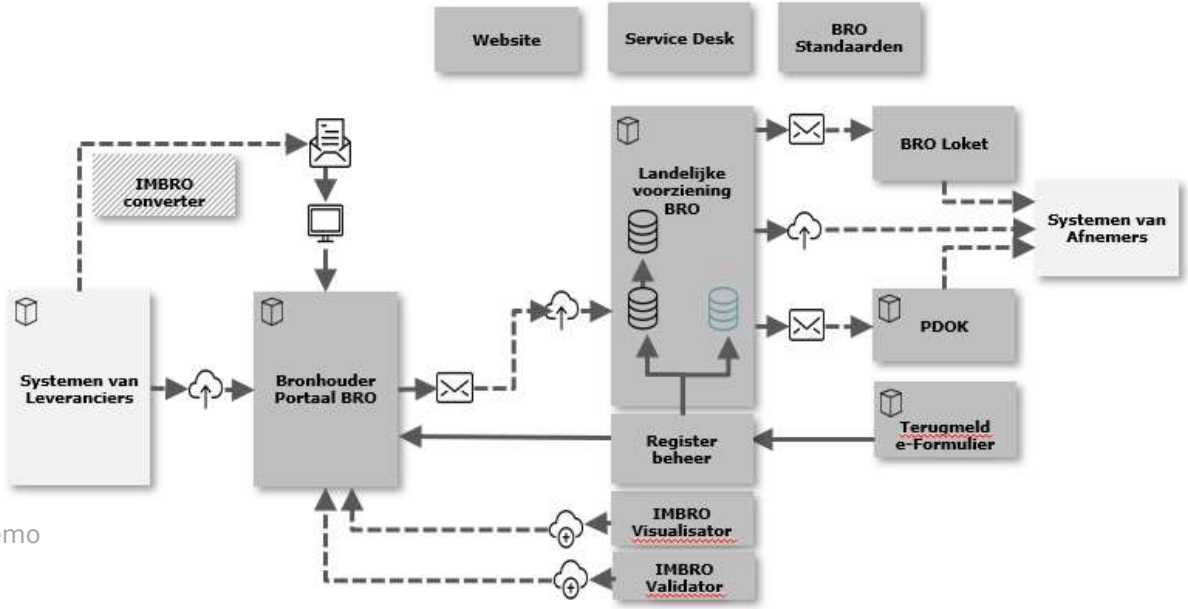
Programma BRO

Basisregistratie Ondergrond

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Welkom, namens de makers van de BRO

TNO



GEONOVUM

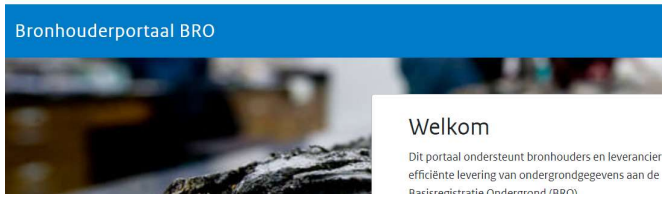
pdok

Doel van de ketendemo

- De makers laten zien wat er in de afgelopen periode is gerealiseerd. (4 weken)

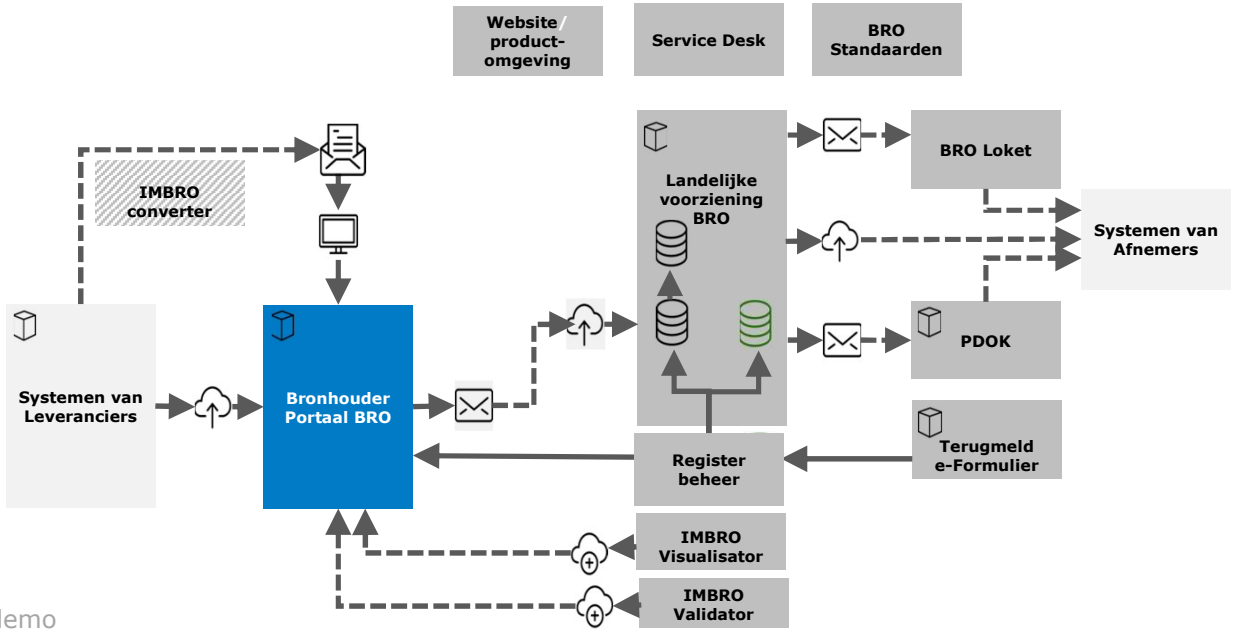
- Doel is:
  - ✓ informeren,
  - ✓ feedback ontvangen,
  - ✓ samenwerking bevorderen

- Voortgang laten zien en vooruitblik komende periode (roadmap)



Vandaag in de BRO Ketendemo

Vorderingen Bronhouderportaal tav security
→ Wijzigingen van machtigingen



Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security van het Bronhouderportaal, wijzigingen tav machtigingen

Jos Nieuwenhuizen | software-ontwikkelaar BRO LV + BHP

Sjaak Derksen | Product Owner BRO LV + BHP

Stephan Gruijters | Product Manager BRO

Randvoorwaarden

- BRO Ketenarchitectuur
  - Authenticatie en autorisatie zijn gescheiden
  - Authenticatie (wie ben ik?)
    - Verplichting te voldoen aan de te ISO/ NORA / BIR
    - Implementatie: E-herkenning en PKI overheid certificaat
  - Autorisatie (wat mag ik?)
    - Op één plek vastleggen

Randvoorwaarden

- Programma Implementatie

Authenticatie en autorisatie door elkaar
NIET compliant
Authenticatie conform BIR
NIET compliant
Autorisatie op twee plekken
NIET compliant

- Implementatie 2023

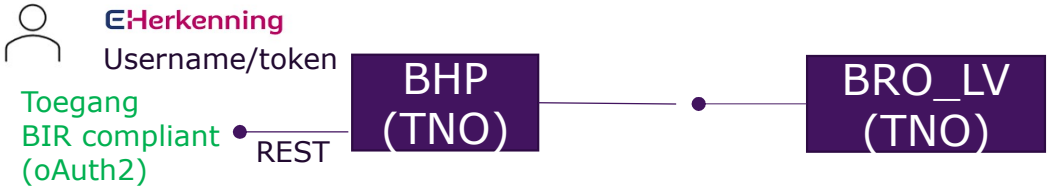
Authenticatie los van autorisatie
Compliant
Authenticatie conform BIR
NIET compliant
Autorisatie op één plek
compliant

Randvoorwaarden

- Implementatie 2023

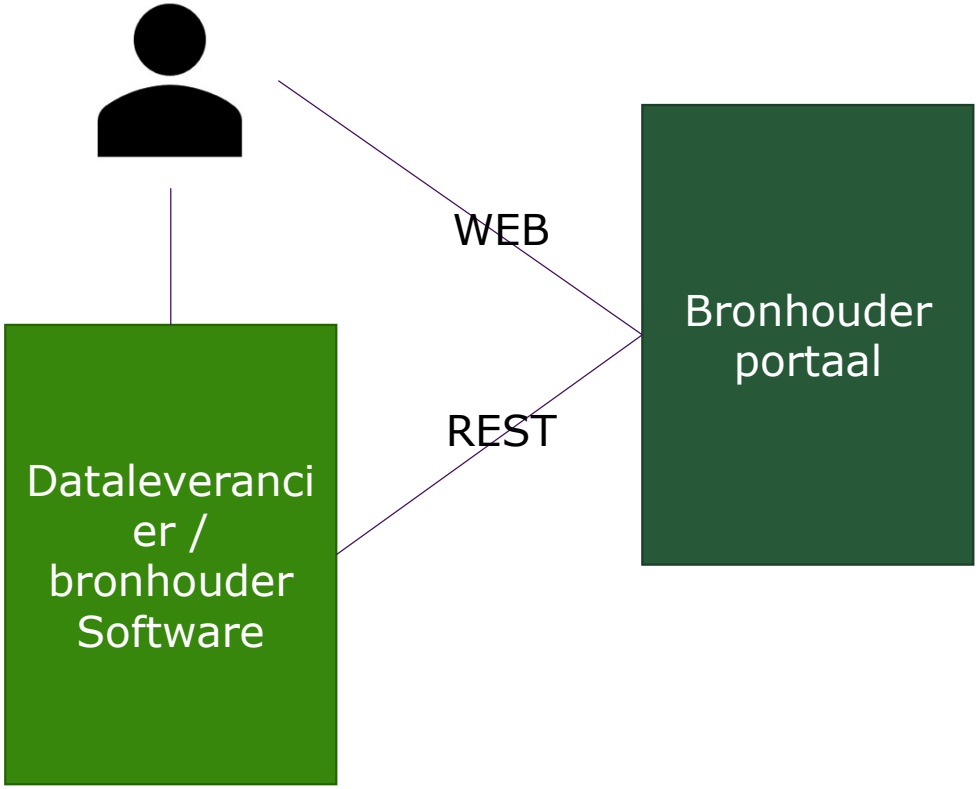
Authenticatie los van autorisatie
compliant
Authenticatie conform BIR
NIET compliant
Autorisatie op één plek
compliant

- Toekomstige Implementatie



Authenticatie los van autorisatie
compliant
Authenticatie conform BIR
compliant
Autorisatie op één plek
compliant

Context



Klaar gedaan

Bezig bezig

Te doen gepland

Waarom nu aanpassingen?

- In den beginne is het bronhouderportaal gemaakt met als uitgangspunt “een zo laagdrempelig mogelijke toegang”.
- Dat heeft er toe geleid, dat iedere project:
  - Meerdere (dezelfde en verschillende typen) machtigingen kan hebben
  - Met in iedere machtiging een token
- Verder zijn er nog afzonderlijke tokens voor “verrijken” en “valideren”
- Gevolg 1: Een grote hoeveelheid tokens die een veiligheidsrisico vormen.
- Gevolg 2: Niet meer te beheren voor dataleveranciers die veel bronhouders bedienen.

Authenticatie en Autorisatie

- Authenticatie: het vaststellen van de identiteit van de gebruiker (stap 1)
- Autorisatie: het vaststellen van de rechten van een gebruiker (stap 2) met als doel het toepassen van die rechten.

- Dit loopt in het huidige bronhouderportaal door elkaar heen:

  - Een token is een vorm van authenticatie!! => Deze behoeft maar éénmaal te worden verstrekt tijdens de uitwisseling van gegevens.
    - Denk bijvoorbeeld aan inloggen op je PC of computernetwerk op het werk.
    - Denk bijvoorbeeld aan je inlogtoken bij een bank.

  - Een machtiging is een vorm van autorisatie!! => Dit wordt continu bekeken na inloggen
    - Bij veel organisaties wordt bepaald aan de hand van wie je bent wat je mag op een PC of computernetwerk.
    - Je mag na inloggen alleen de rekeningen zien waartoe je bent geautoriseerd. Bijvoorbeeld, die van jezelf, je partner en je kinderen.

Terug naar één token?

- Stap 1. Terug naar één machtiging per dataleverancier per project.
  - A) De meest logische stap om het aantal tokens terug te dringen is terug naar één machtiging per project. Dit is reeds uitgevoerd. Het is niet meer mogelijk om meerdere machtigingen voor dezelfde leverancier aan te maken binnen één project. ☑
  - B) Daarna de bestaande situatie van meerdere machtigingen per project (per dataleverancier) één voor één aanpakken. Dit betekent contact zoeken met de desbetreffende bronhouder (servicedesk) en machtigingen sluiten. ☑
  - C) Opties binnen een machtiging uitbreiden (filtering per registratie object mogelijk) ☐

Terug naar één token?

- Stap 2. Authenticatie en Autorisatie uit elkaar halen.
  - Er is een nieuwe URL beschikbaar voor het leveren op het bronhouderportaal vanuit de software

    Een voorbeeld: `/api/v2/{project_id}/leveringen` ☑
  - Dit stelt softwareleveranciers in staat om hun software geleidelijk aan te passen

Terug naar één token?

- Stap 3b. Één token ☐
  - Het token uit de machtiging halen en naar de omgeving (in het bronhouderportaal) van de dataleverancier brengen.
  - Voor nieuwe leveranciers kan dit relatief snel.
  - Voor bestaande leveranciers moet hiervoor de nieuwe URL worden gebruikt. Anders kunnen wij niet meer vaststellen voor welk project de levering plaats vindt.
  - Zodra wij constateren dat de nieuwe URL door een dataleverancier wordt gebruikt kunnen wij met behulp van een “wizzard” migratie voorstellen.

Terug naar één token?

- Stap 3a. Één token ☑
  - Onze software moet hier ook klaar voor zijn. Daarom zijn wij in de tussenliggende tijd “onder de motorkap” bezig onze software aan te passen.

Terug naar één token?

- Stap 4. Uit faseren huidige situatie ☐
  - De overheidsrichtlijnen (BIR / NORA) stellen dat tokens een beperkte geldigheid moeten krijgen.
  - Dit wordt op enig moment toegepast voor de nieuwe situatie.
  - Maar ook voor de oude situatie.
  - De verwachting is dat alle softwareleveranciers op enig moment over zijn op de nieuwe (v2) URL. Dan kunnen wij dit project afronden.

Terug naar één token?

- Stap 5. Toekomst ☐
  - Het centraal managen authenticatie biedt nieuwe mogelijkheden. Zoals het overgaan op authenticatiemiddelen die op de pas-toe-of-leg-uit lijst van onze overheid zijn opgenomen (oAuth2).
  - Uiteindelijk willen we geleidelijk afstand nemen van JWT Tokens en overgaan op deze manier van authenticeren.

En verder

- Ook de huidige inlog mogelijkheden op het bronhouderportaal web worden beperkt en in lijn met BIR / NORA gebracht.
- “Alleen gebruikersnaam / wachtwoord” gaat verdwijnen.
- Overgebleven mogelijkheden:
  - 2 factor authenticatie: gebruikersnaam + gegenereerd token (app)
  - E-Herkenning

DEMO

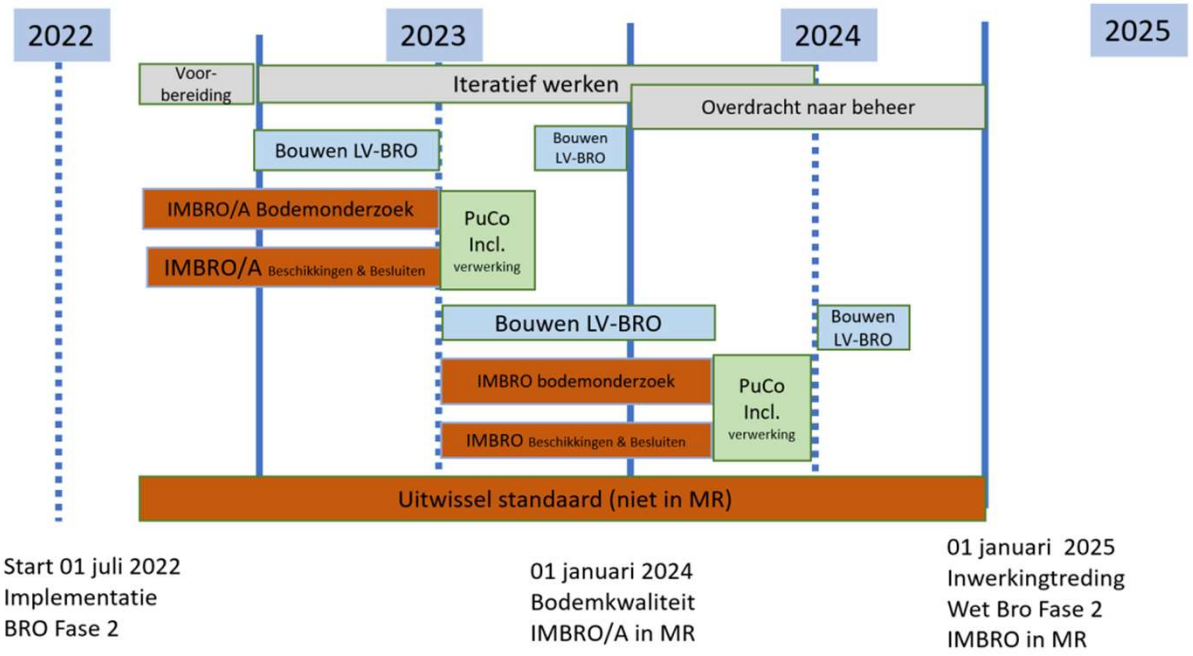
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

BRO roadmap

Roadmap Milieukwaliteit (fase II)

Planning en doorlooptijd standaarden

Tranche fase 2 : wetgevingscyclus ca. 18 maanden doorlooptijd

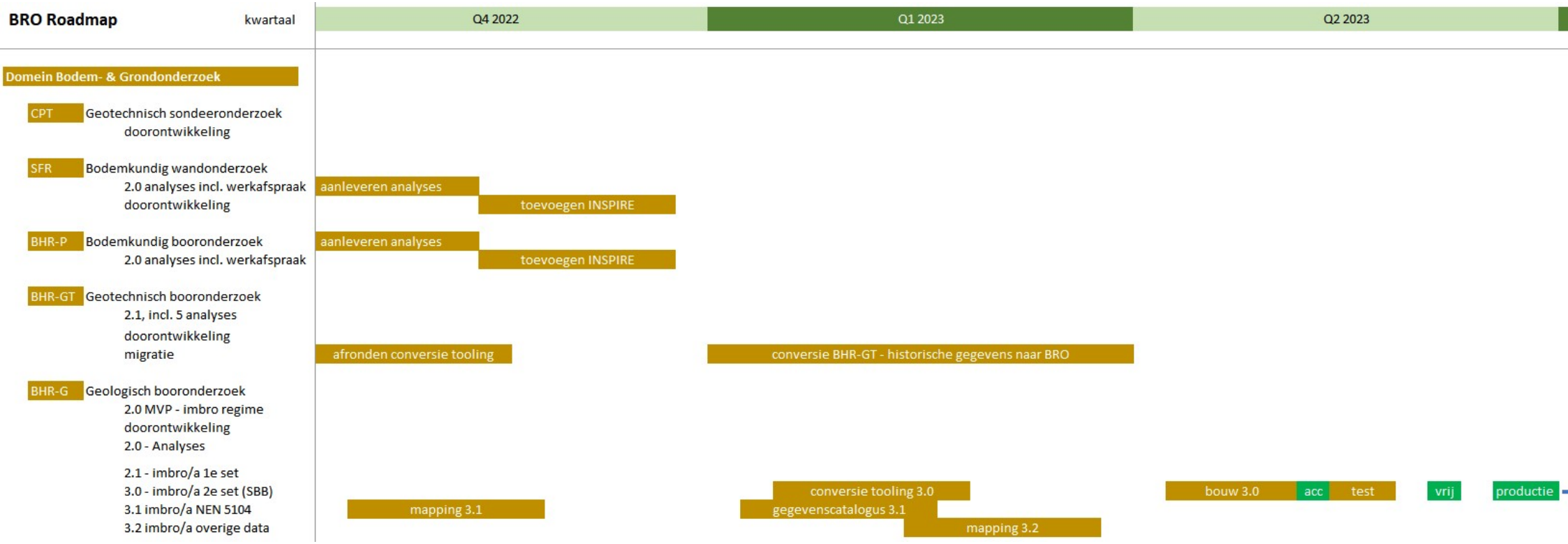


Start 01 juli 2022
Implementatie
BRO Fase 2

01 januari 2024
Bodemkwaliteit
IMBRO/A in MR

01 januari 2025
Inwerkingtreding
Wet Bro Fase 2
IMBRO in MR

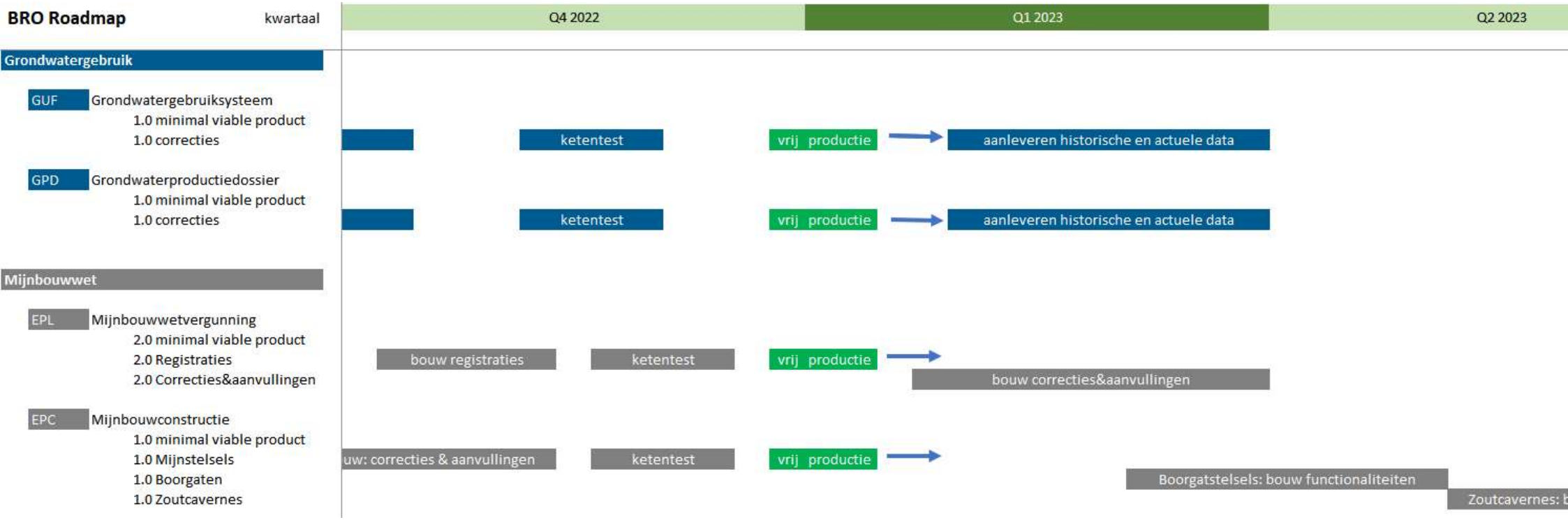
Gepland werk Q4



Gepland werk Q4

BRO Roadmap	kwartaal	Q4 2022	Q1 2023	Q2 2023	
Domein Grondwatermonitoring					
GMW	Grondwatermonitoringput doorontwikkeling		uitbreiding standaard, oa niet openbaarheid en koppeling boring	publ. consultatie catalogus	
GMN	Grondwatermonitoringnet doorontwikkeling				
GAR	Grondwatersamenstellingsonderzoek doorontwikkeling			publ. consultatie catalogus	migratie historische data
GLD	Grondwaterstandonderzoek doorontwikkeling		afronden migratie historische data naar de BRO	publ. consultatie catalogus	
FRD	Formatieweerstandonderzoek 1.0 basis services doorontwikkeling				

Gepland werk Q4



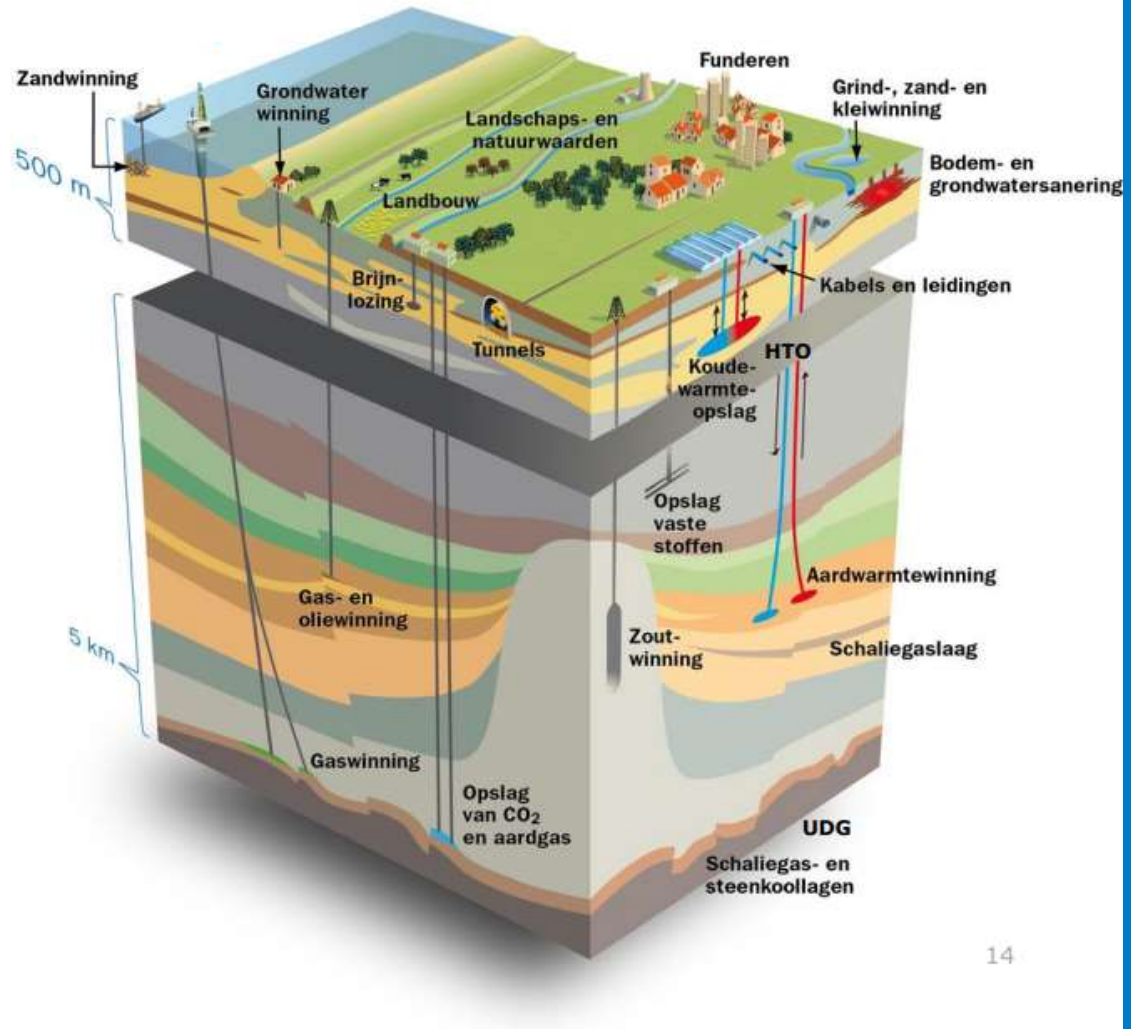
Gepland werk Q4

BRO Roadmap	kwartaal	Q4 2022	Q1 2023
BRO systeem preventief beheer			
		Security: verminderen tokens in omloop	
		Identificatie en authenticatiemanagement voor notificaties	
		start vervangen eHerkenning	
		CPT in Enterprise Architecture	
		Openshift omgeving in nieuwe datacenter	

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

BRO Nieuws en reminders:

- Sprintreview BRO standaard Milieukwaliteit, maandag 19 dec.
- Stelseldag, 28 november
- BRO’tje 15 december a.s
- 1 januari: weer een nieuw jaar



Dank en tot ziens!