

Effectieve start om 13u05!

Uitfasering Geosecure

**Stappenplan voor API-client
migratie**

INFOSESSIE 19 januari 2023



**DIGITAAL
VLAANDEREN**



**Vlaamse
overheid**

AGENDA

Start opname van de infosessie



- Opname & slides zullen worden voorzien na de infosessie
- Vragen zullen beantwoord worden tijdens het vragen moment...
- Gelieve camera en microfoon tijdelijk uit te schakelen aub

Voorstelling – Wie zijn wij?

Geert Lauwaert – Project Manager



Liesbeth Rombouts – Product Owner
Geosecure en KLIP



Sammy Roos – Product Owner
Toegangsbeheer (ACM)



Wie zijn jullie en voor wie is deze INFOSESSIE?

✓ Iedereen die in Geosecure eigenaar is van een API-client: de eindklant of een dienstenleverancier

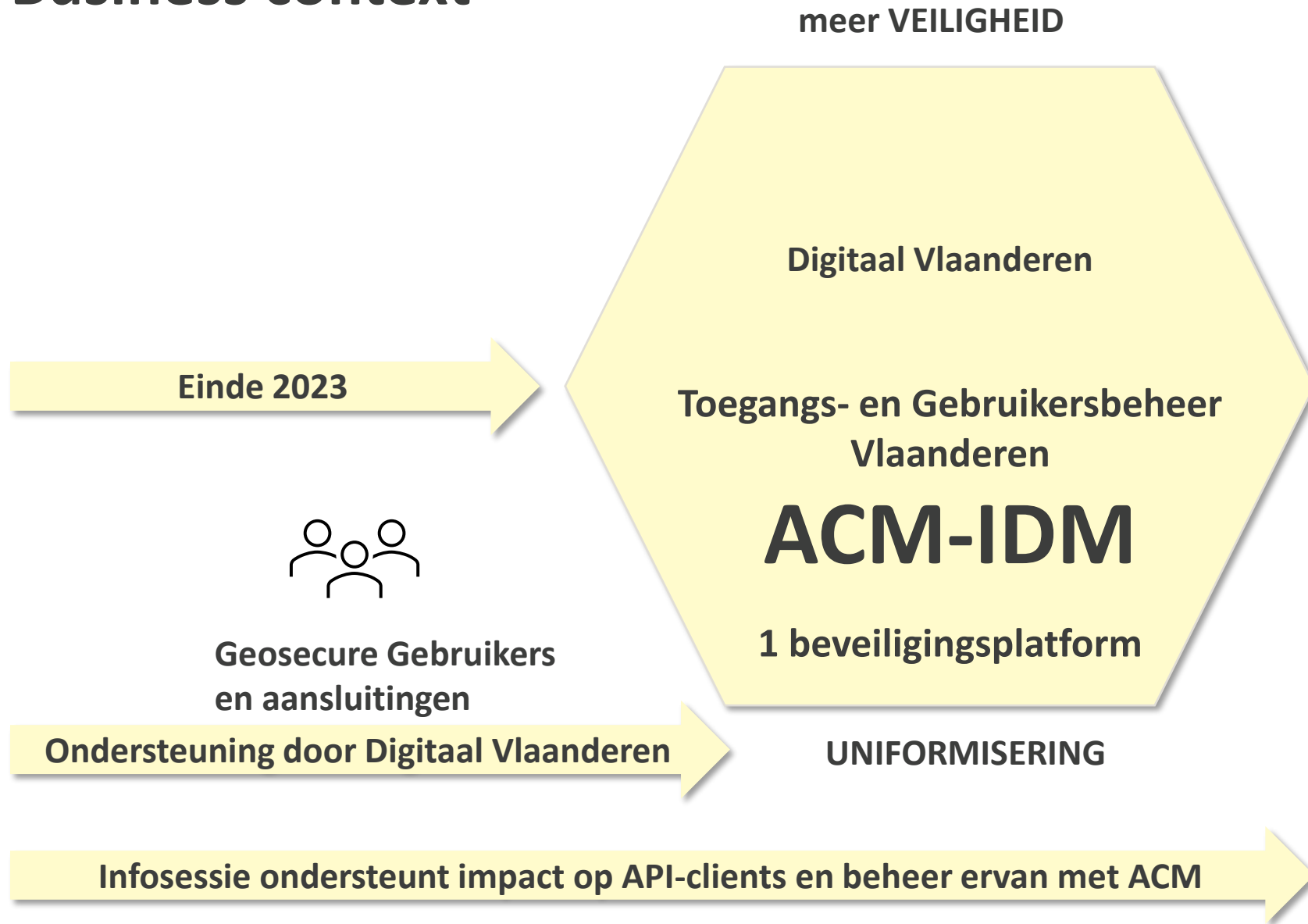
✓ Iedereen die toelichting wil over de API-clients migratie en aansluiting op het Toegangsbeheer (ACM)

❖ NIET voor eigenaars van API-clients voor MAGDA
MAGDA team doet dit zelf

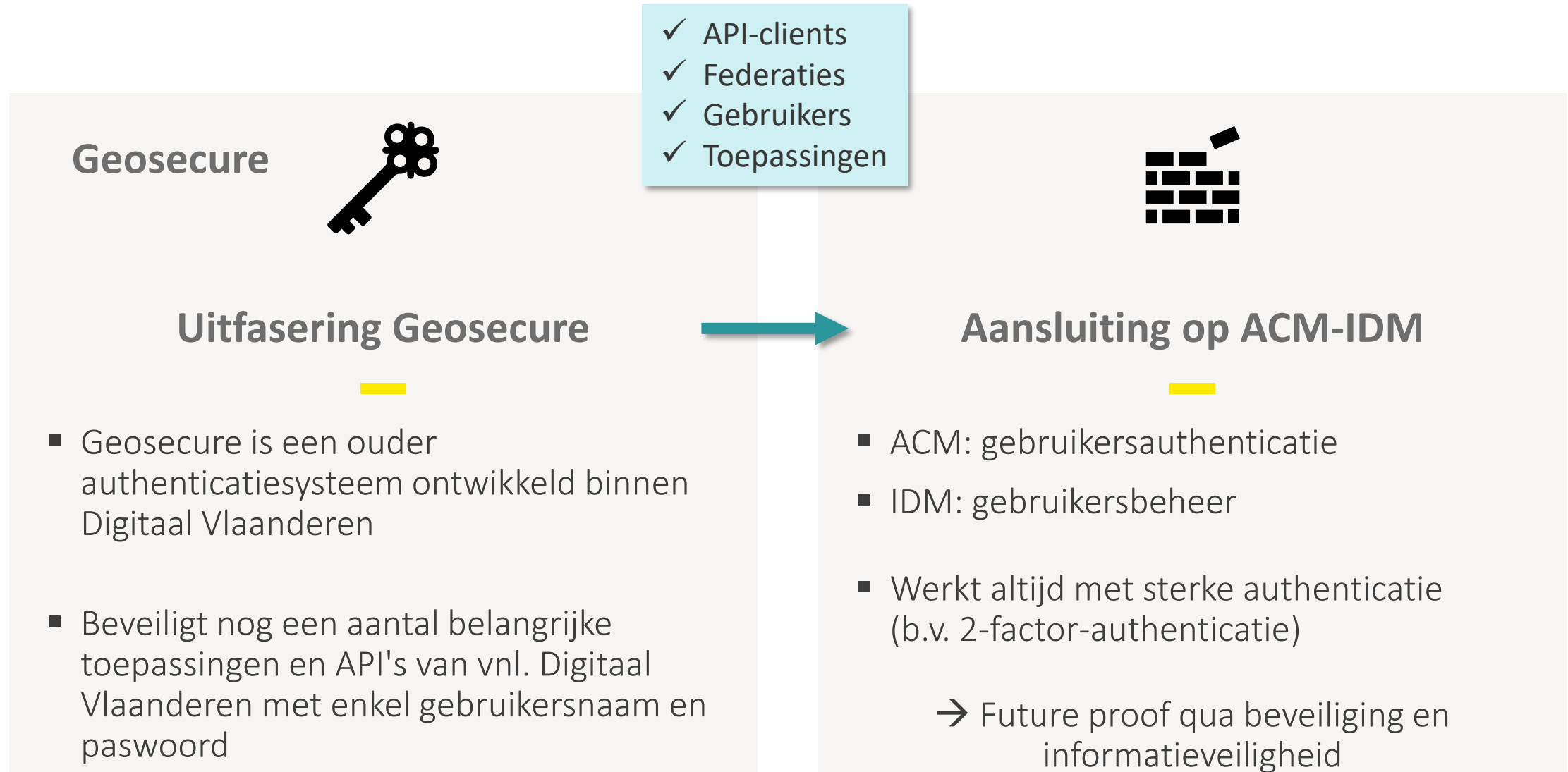
Agenda

- | | |
|--|-----------------|
| 1. Business context en doelstelling project | 13:00 tot 13:20 |
| Aanpak en tijdslijn project | |
| Vragen? | 13:20 tot 13:45 |
|
 | |
| 2. Scenario's voor overschakeling van de API-clients | 13:45 tot 14:30 |
| Vragen? | 14:30 tot 15:00 |
|
 | |
| Korte pauze 5' | |
|
 | |
| 3. Demo ACM Selfservice Portaal voor API-clients | 15:00 tot 15:30 |
| Vragen? | 15:30 tot 16:00 |

Business context



Doelstelling van het project Uitfasering Geosecure



Doelstelling van het project Uitfasering Geosecure

Wie doet wat?

- ✓ API-clients
- ✓ Federaties
- ✓ Gebruikers
- ✓ Toepassingen

Digitaal Vlaanderen

Migratie en aansluiten van alle **Gebruikers** en **Toepassingen** van Geosecure naar ACM.

Ondersteuning

API-client Beheerders

Overschakelen van hun **API-Clients** naar ACM.

Gefedereerde Organisaties

Opzetten nieuwe federatie voor hun **IDP** met ACM.



Aanpak

4 PARALLELE TRAJECTEN EN EEN COMMUNICATIEPROGRAMMA

Traject 1

- Migratie **fysieke gebruikers**

Traject 2

- Migratie **API-Clients**

Traject 3

- Migratie **toepassingen** met **transitiefase** voor overschakeling API-Clients en Federaties

Traject 4

- Migratie **toepassingen** door vernieuwingsprojecten

Communicatieprogramma “Van Geosecure naar Toegangsbeheer Vlaanderen ACM-IDM”

Aanpak: focus infosessie

4 PARALLELE TRAJECTEN EN EEN COMMUNICATIEPROGRAMMA

Traject 1

- Migratie fysieke gebruikers

Traject 2

- Migratie **API-Clients**

Traject 3

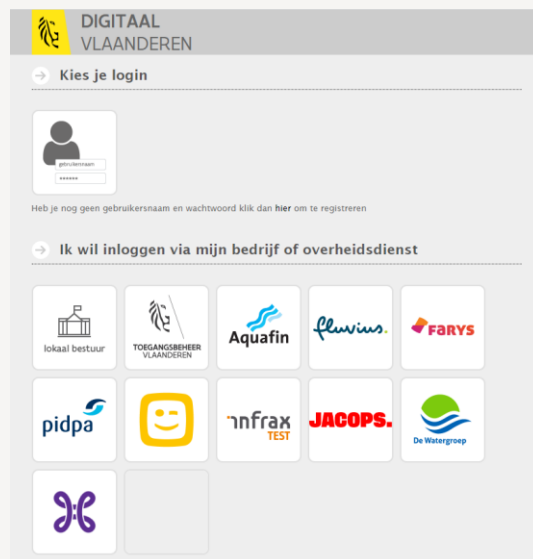
- Migratie **toepassingen** met **transitiefase** en overschakeling API-clients

Traject 4

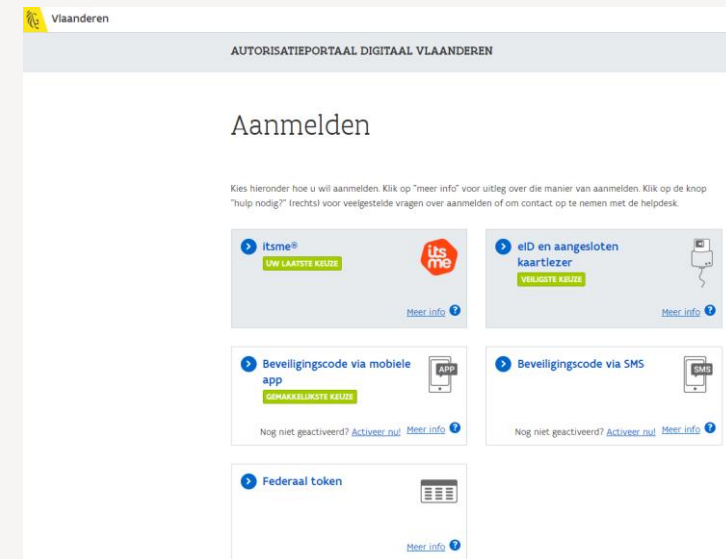
- Migratie toepassingen door vernieuwingsprojecten

Migratie fysieke gebruikers: 2023

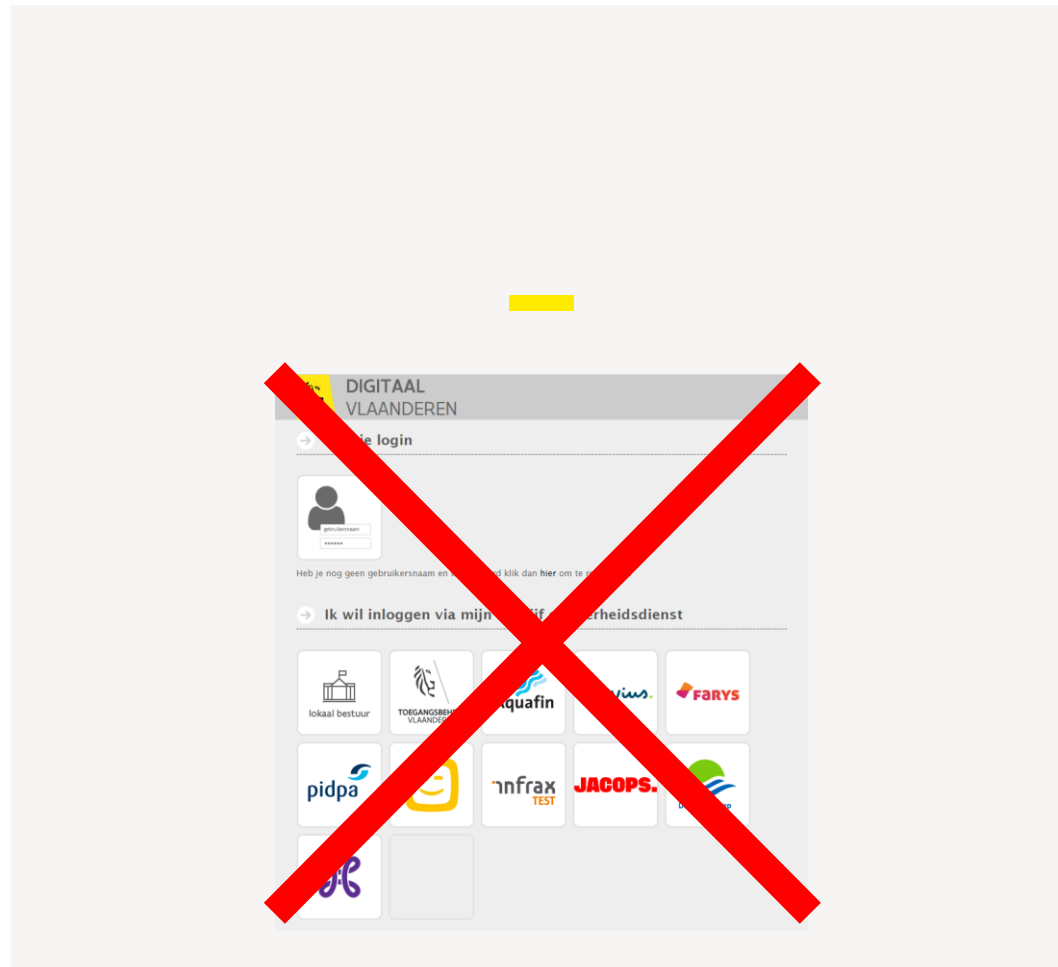
Nog mogelijk in 2023



Wordt ook mogelijk vanaf 2023



Migratie fysieke gebruikers: vanaf 2024



Migratie API-clients: geplande stappen

Kickoff: deze infosessie

Toepassing wordt in TEST of PRD aangesloten op ACM

Communicatie wordt gestuurd “**toepassing in transitiefase**” + **API-Client info**:

- welke API-clients zijn in bulk gemigreerd en wat doen om die aan te sluiten op ACM
- welke API-clients 1 per 1 opgezet moeten worden door de API-beheerder

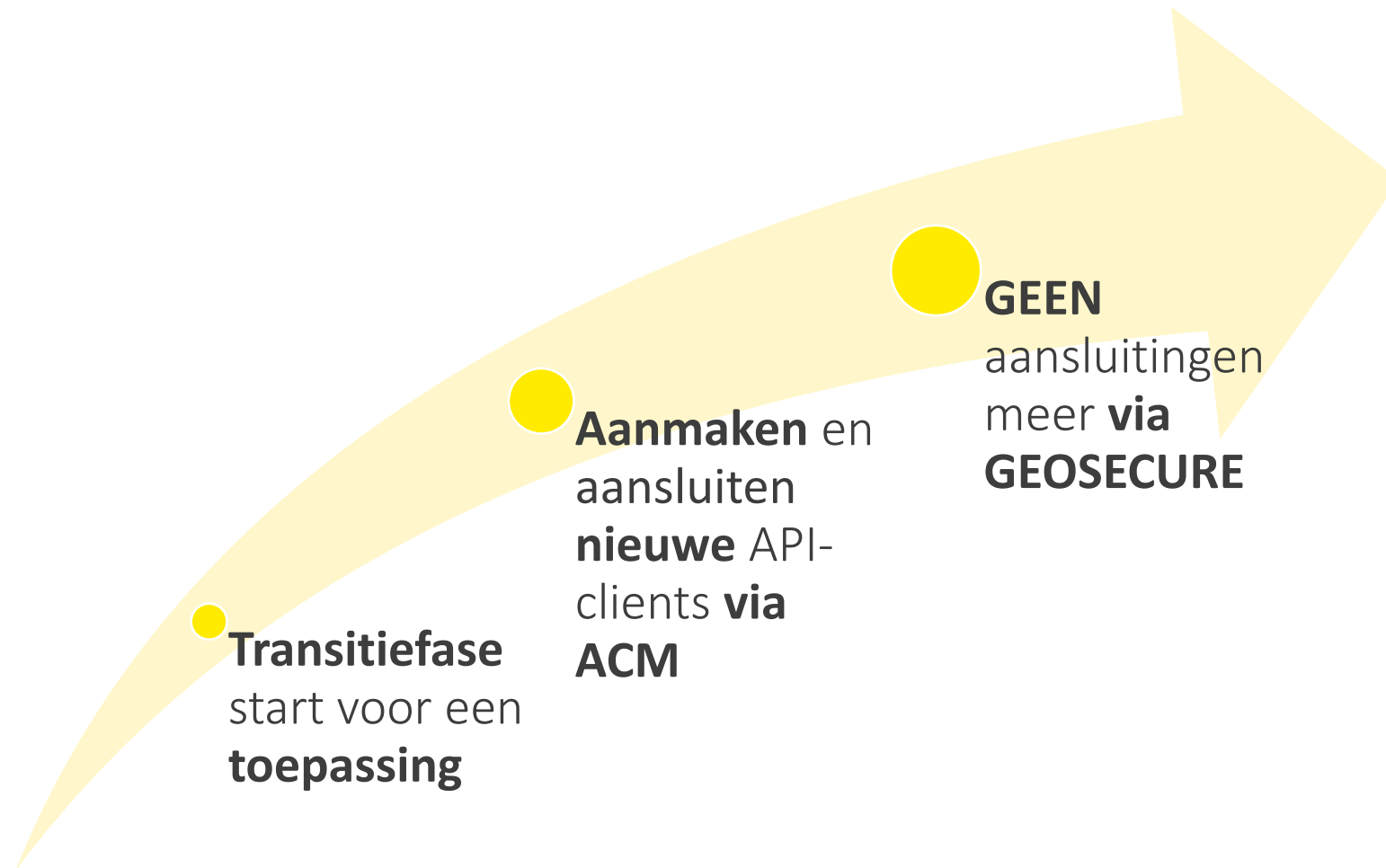
De **transitiefase** duurt maximaal **tot einde 2023** → alle **API-Clients** moeten overgeschakeld zijn naar ACM

Belangrijk weetje: Tijdens de **transitiefase** zullen **API-clients** zowel met **Geosecure** als met **ACM** aangesloten kunnen zijn

Migratie API-clients: omgevingen



Migratie API-clients: nieuwe aansluitingen



Migratie toepassingen met transitiefase voor overschakeling API-clients

Toepassingen die migreren



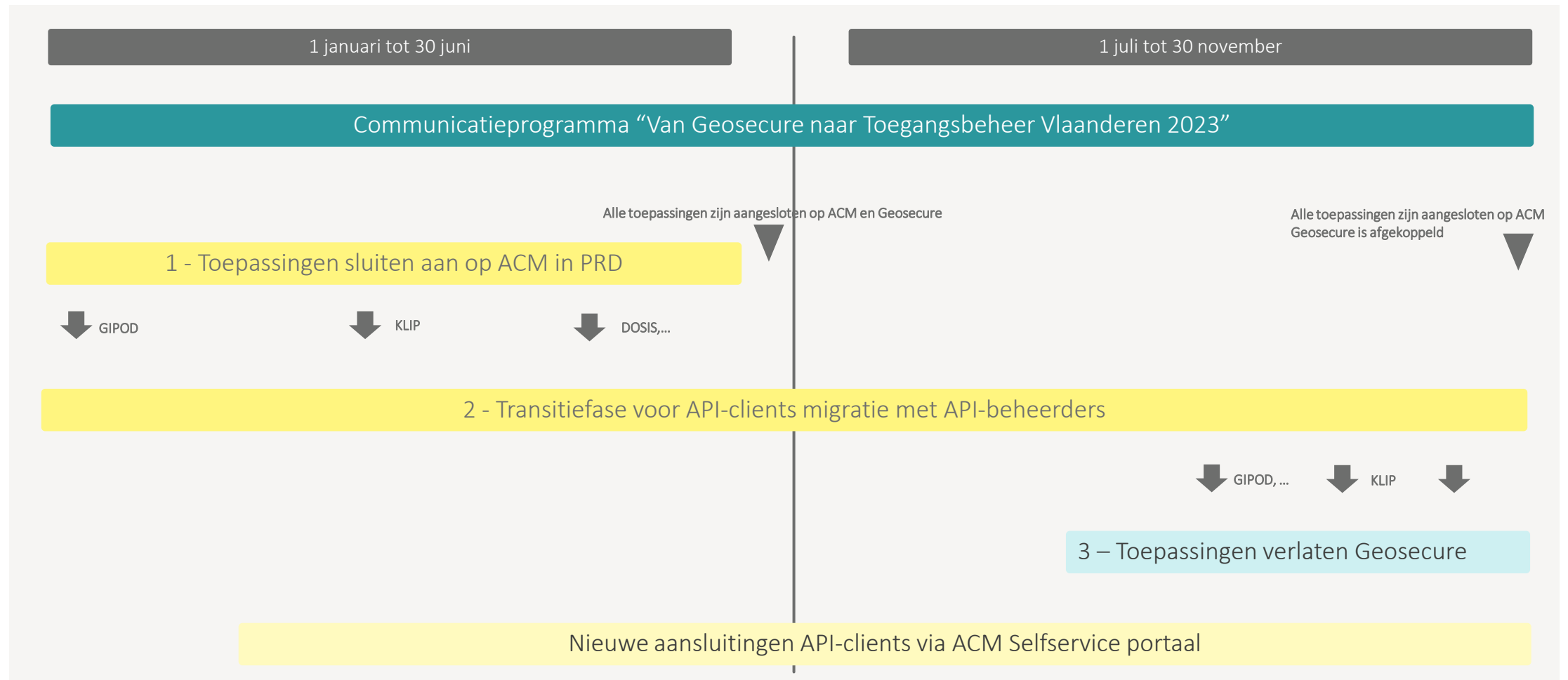
- Metadata Vlaanderen en Metadatacenter
- GRB/GECKO
- GTMF/Meldingen
- MAGDA
- KLIP
- GIPOD
- Mijn Burgerprofiel
- Dosis
- Notificaties

Volledig vernieuwde toepassingen



- RVV
- CRAB/LARA
- DataPublicatie/PBS3000
- Download
- Geopunt

Tijdslijn 2023



Communicatieprogramma “Van Geosecure naar Toegangsbeheer Vlaanderen ACM-IDM”

Doelstelling: Migratie naar ACM-IDM zo vlot mogelijk laten verlopen.

- Zelfregistratie tienduizenden gebruikers op gang trekken en zo naadloos mogelijk opvolgen en afwerken.
- Ervoor zorgen dat alle betrokkenen gebruikers, agentschappen, bedrijven, ...
 - zo goed mogelijk geïnformeerd zijn,
 - de noodzaak van de migratie begrijpen
 - inzicht en kennis verwerven over de nieuwe sterke aanmelding via ACM-IDM

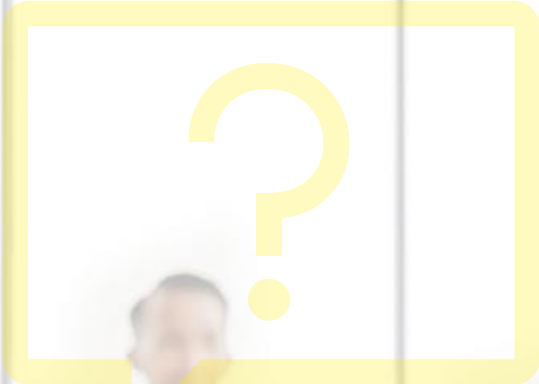


Gebruikersnaam en paswoord van Geosecure maken plaats voor 2-factor authenticatie van ACM-IDM

Alle toepassingen die vandaag nog via het beveiligingssysteem Geosecure lopen, zullen vóór 1 januari 2024 moeten omschakelen naar ACM-IDM. Digitaal Vlaanderen kiest immers voor de veiligere 2-factor authenticatie van toegangs- en gebruikersbeheer Vlaanderen (ACM-IDM). Daarbij doorloopt u telkens twee stappen voor u toegang krijgt. Wie moet overschakelen wordt gecontacteerd door Digitaal Vlaanderen en krijgt de nodige ondersteuning. [Meer informatie vindt u in het nieuwsbericht.](#)

Communicatie en informatiekanalen:

- Info en FAQ: [Migratie van API-clients van Geosecure naar ACM](#)
- Stel uw vraag via onze mailbox uitfaseringgeosecure@vlaanderen.be
- **Nieuwsbrieven**, nog niet ingeschreven > Schrijf u in! [Via deze link](#)
Gisteren is een artikel in de Nieuwsbrief van Digitaal Vlaanderen verschenen [Meer informatie vindt u in het nieuwsbericht.](#)
- **Landingspagina** op site van Digitaal Vlaanderen "Van Geosecure naar Toegangsbeheer Vlaanderen ACM-IDM" met informatie en status over uitvoering en planning [Via deze link](#)



Vragen?



Scenario's voor overschakeling van de API-clients

Structuur

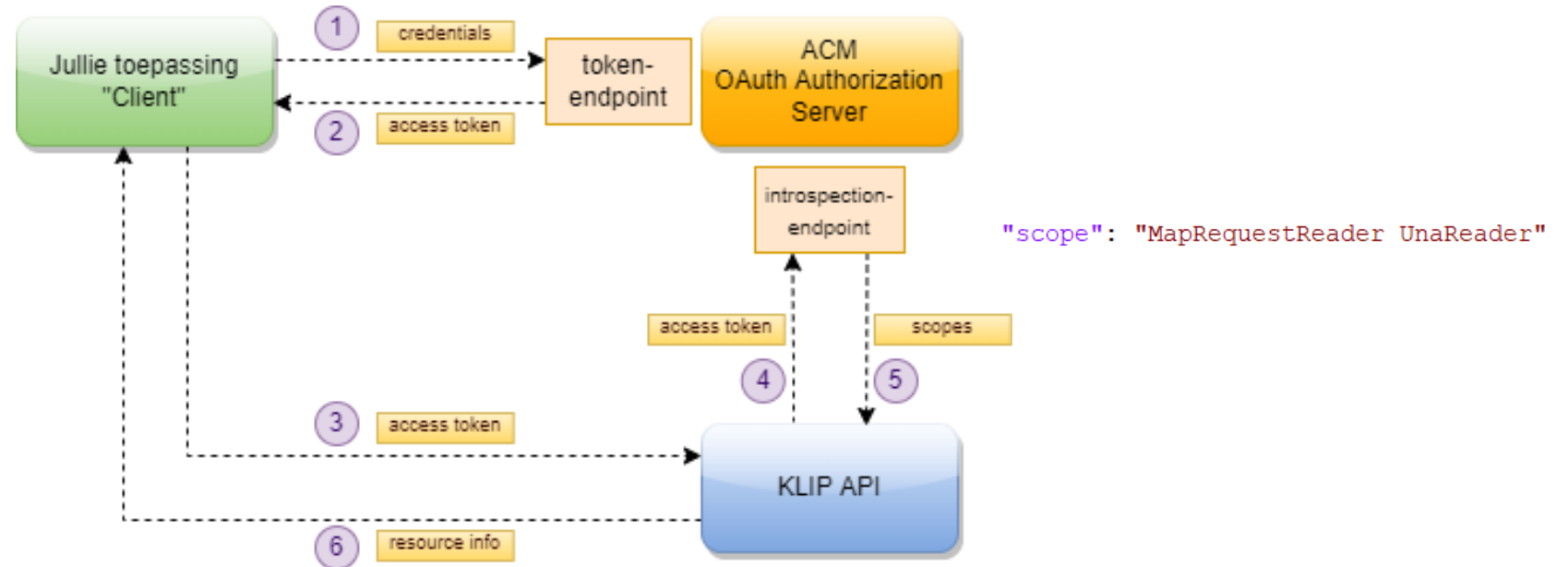
Wat gaan we overlopen in dit onderdeel:

- Terminologie: Clients, API's, JWK's, enz.
- Algemene principes bij de migratie
 - Bulk migratie van de Clients waar mogelijk
 - Gebruik van het ACM Selfservice Portaal
- Wat verandert er wel/niet t.o.v. de oude situatie met Geosecure
- Overlopen van de verschillende scenario's waar klanten zich kunnen in bevinden

Terminologie: Clients, API's en ACM OAuth

Vereenvoudigd schema van een REST API-connectie beveiligd via OAuth

```
"access_token": "Geh30TieWrbRdlsnCLDJDezs63ne2djd8eSxhznd5b",  
"token_type": "Bearer",  
"expires_in": 3600
```



Terminologie: wat is een JWK?

Bij de aanvraag van een token moet een Client zijn identiteit bewijzen (authenticatie):

- Met zijn ClientID en een *shared secret*
- Of met zijn ClientID en een JSON Web Key (JWK) -> meest veilige optie

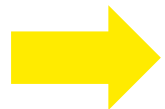
Een JSON Web Key is een **sleutelpaar (private sleutel en publieke sleutel)** waarmee je bepaalde gegevens kan encrypteren of handtekenen. In onze API-stroom wordt het gebruikt om **je tokenaanvraag te handtekenen** (= bewijzen dat jij de afzender bent)

- Je slaat de private sleutel veilig op binnen je toepassing
- Je bezorgt aan ACM de publieke sleutel
- Bij je tokenaanvraag onderteken je je aanvraag (JWT) met je private sleutel
- **ACM verifieert je handtekening met de aangeleverde publieke sleutel**

Algemene principes: bulkmigratie

Waar mogelijk gaan we de gegevens uit Geosecure eenmalig overzetten naar het Toegangsbeheer (ACM) in bulk

- Aanmaken van de Client (met de bijhorende gegevens)
- Koppelen van de Client met de juiste API (en bijhorende scopes)
- Overnemen van de JWK (indien beschikbaar)



Vereenvoudiging van de migratiestappen in bepaalde scenario's

Sommige stappen of scenario's zullen echter nog steeds acties van de klant vragen

- In sommige scenario's zal de klant zelf de Client moeten aanmaken, koppelen met de API, enz.
- In elk scenario zal de klant bepaalde acties langs zijn kant moeten doen (zie verder: endpoints aanpassen, ClientID's aanpassen, enz.)

Algemene principes: ACM Selfservice Portaal

ACM Selfservice Portaal (“Beheerportaal”): webtoepassing waar klanten van het Toegangsbeheer zelf (in selfservice) bepaalde acties kunnen doen

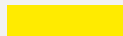
- API- en Clientbeheer: creëer en beheer zelf Clients (in T&I en PRD) voor een bepaalde API
- Diverse workflows tussen klanten en dienstverleners (goedkeuring, delegatie, enz.)
- Instellen van toegang via het Gebruikersbeheer van de Vlaamse overheid (IDM): specifiek recht “API-beheerder” (of toegang als wettelijk vertegenwoordiger)

Acties van klanten voor de Geosecure-migratie zullen **zoveel als mogelijk via het ACM Selfservice Portaal gebeuren**

- Aanmaken en beheren van Clients (indien geen bulkmigratie mogelijk)
- Consulteren van informatie over gemigreerde Clients

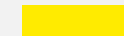
Wat verandert wel/niet?

Blijft hetzelfde



- **Endpoints en structuur van de Business API's**
 - Aan de API's (b.v. KLIP, GIPOD) zelf verandert niets, enkel aan de beveiliging achter de API's
- **Scopes van de API's**
 - Waar mogelijk letterlijk overgenomen
 - Clients kunnen nog steeds dezelfde scopes als vroeger gebruiken
- **JWK's van de Clients (indien gebruikt)**
 - JWK is een publieke sleutel en kan worden gemigreerd naar het Toegangsbeheer

Verandert



- **ClientID's (unieke ID van een Client)**
 - ACM gebruikt UUID's, Geosecure Integers
 - Oude Geosecure ID wordt wel meegenomen als apart veld (niet relevant voor klant)
- **Secrets van de Clients (indien gebruikt)**
 - *Shared secret*, zit niet in de migratie
 - Keuze om voortaan met JWK's te werken
- **Endpoints en communicatie met de OAuth Authorization Server**
 - ACM heeft andere token endpoints
 - Afhankelijk van scenario: afwijkingen in structuur van de calls naar token endpoint

Introductie bij de verschillende scenario's (1)

De huidige Clients in Geosecure gebruiken in hoofdzaak 2 OAuth-flows:

- **Client Credential Grant:** clients die namens eigen organisatie calls doen (1 Client voor 1 organisatie), ca. 95% van totale aantal Clients
 - ✓ Wordt ondersteund op dezelfde manier als in Geosecure
- **Authorization Code Grant (in B2B-variant):** Clients die in naam van verschillende organisaties calls doen (1 Client voor verschillende organisaties, b.v. dienstverlener), ca. 5% van totale aantal Clients
 - ✗ Wordt niet op dezelfde manier ondersteund via ACM. Overschakeling naar Client Credential Grant (1 aparte CCG-Client per klant).

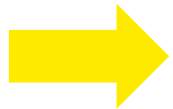
Daarnaast gebruiken ze 2 methodes van authenticatie (van de Client):

- **JWK** (JSON Web Key): ca. 83% van totale aantal Clients
 - ✓ Wordt ondersteund op dezelfde manier als in Geosecure
- **Client Secret** (*shared secret*): ca. 17% van totale aantal Clients
 - ✗ Keuze om niet meer met Client Secrets te werken

Introductie bij de verschillende scenario's (2)

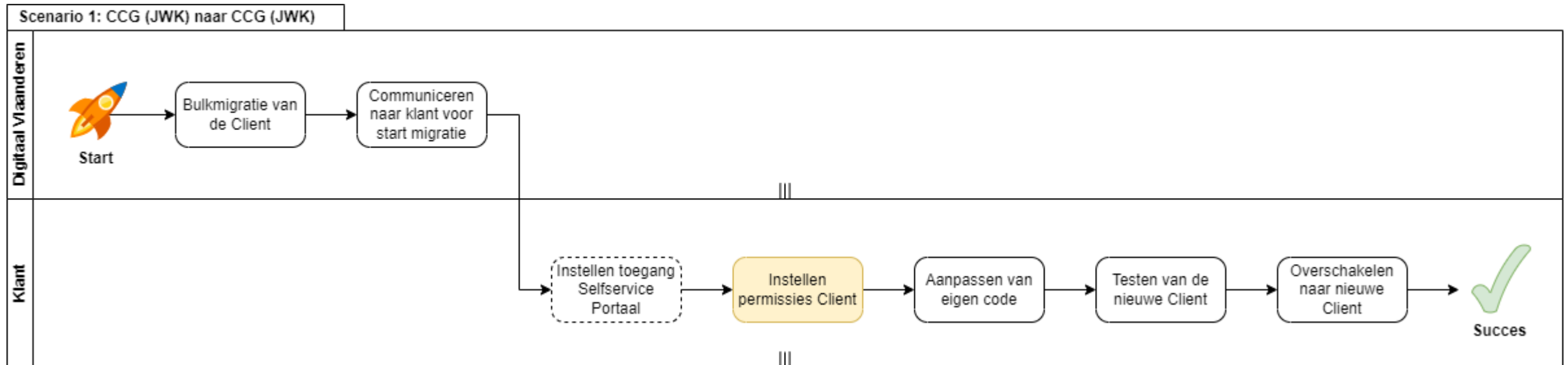
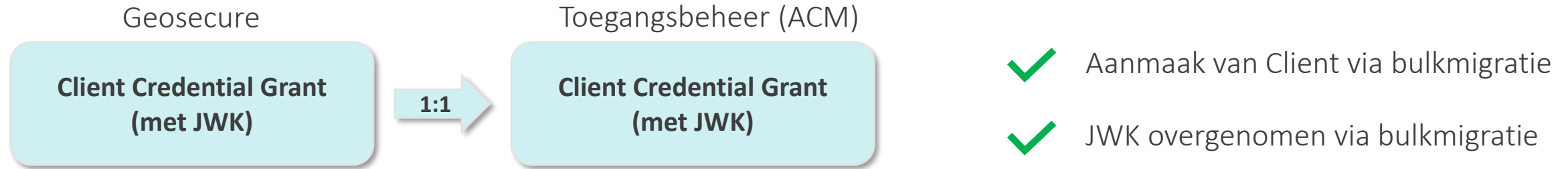
Op basis daarvan hebben we 4 scenario's onderscheiden waarin klanten momenteel kunnen zitten:

- Scenario 1: je gebruikt Client Credential Grant (CCG) met een JWK
- Scenario 2: je gebruikt Client Credential Grant (CCG) met een Secret
- Scenario 3: je gebruikt Authorization Code Grant B2B (ACG) met een JWK
- Scenario 4: je gebruikt Authorization Code Grant B2B (ACG) met een Secret



Verschillende scenario's vragen een verschillende migratieaanpak van de klant

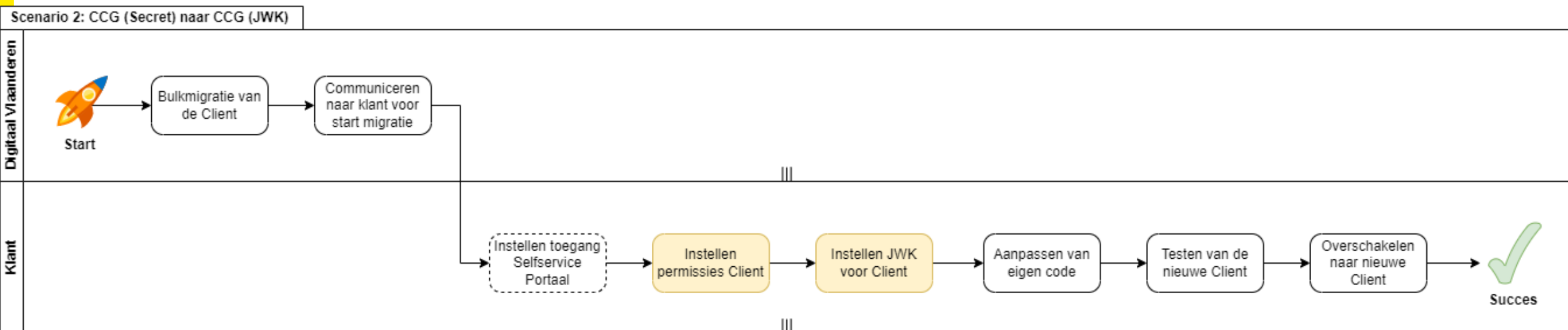
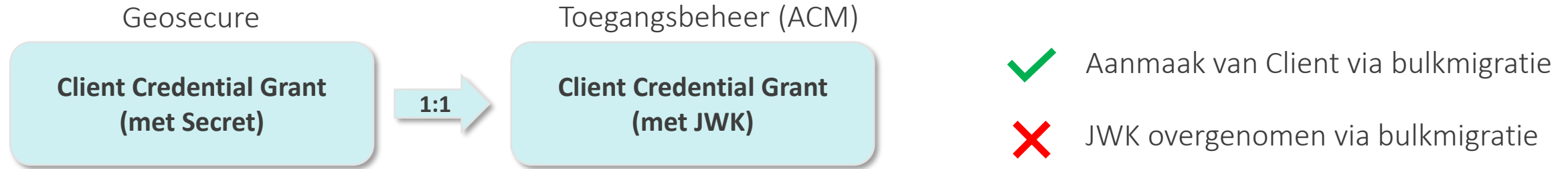
Scenario 1: Client Credential Grant (JWK)



Enmalige acties per organisatie (niet per Client)

Acties in het ACM Selfservice Portaal

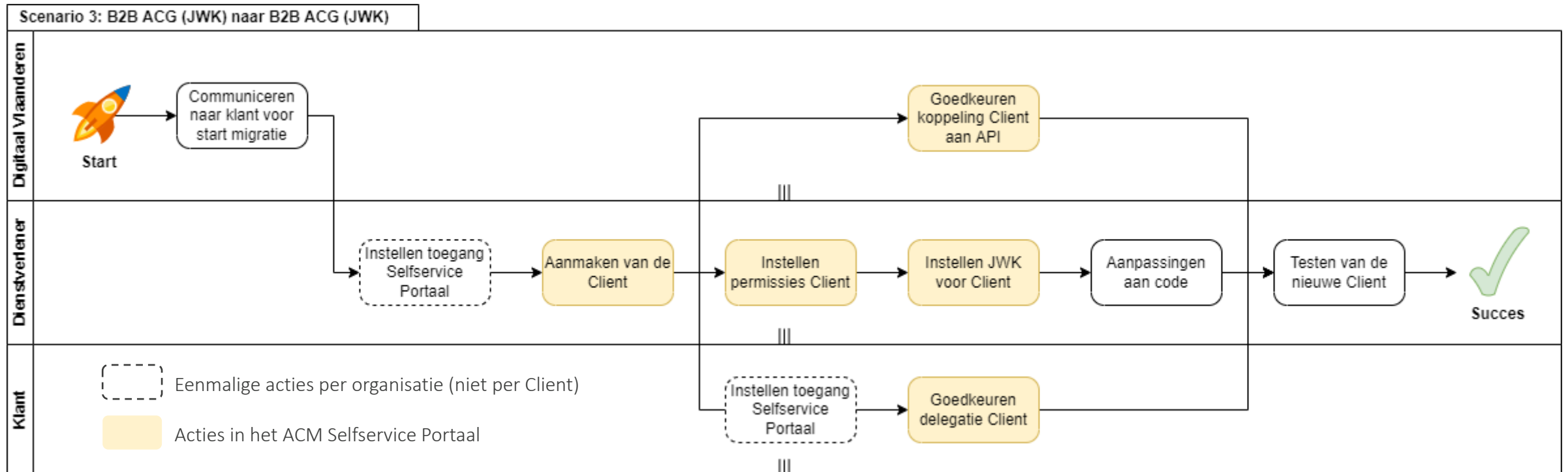
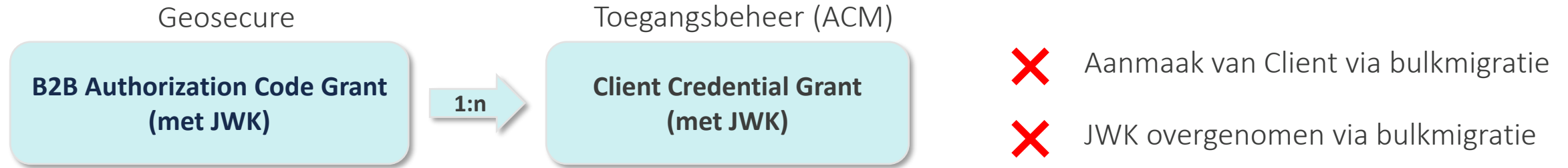
Scenario 2: Client Credential Grant (Secret)



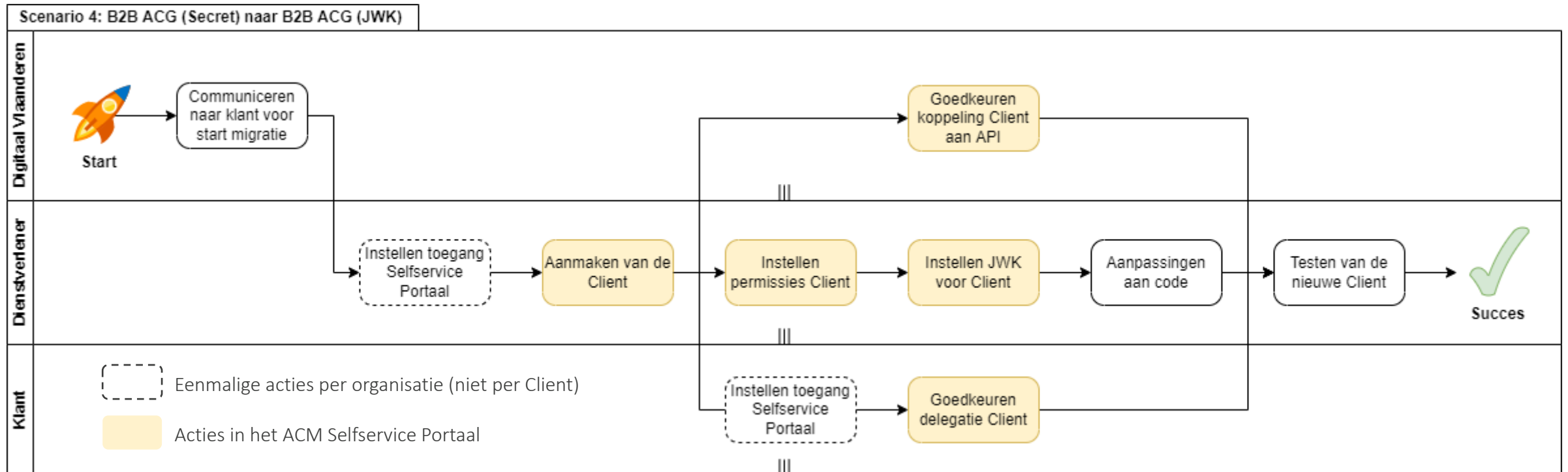
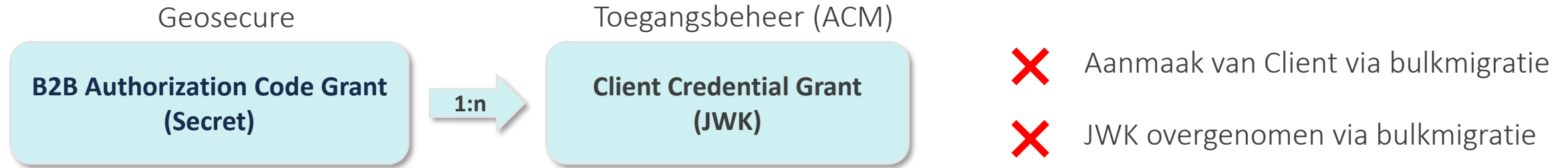
 Eenmalige acties per organisatie (niet per Client)

 Acties in het ACM Selfservice Portaal

Scenario 3: B2B Authorization Code Grant (JWK)



Scenario 4: B2B Authorization Code Grant (Secret)

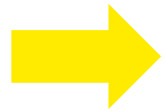


Andere scenario's?

Deze 4 scenario's **dekken 99% van de gevallen** in de migratie van API-Clients

Er zijn mogelijk een aantal **uitzonderingen** die niet onder deze scenario's vallen

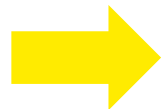
- Standaard Authorization Code Grant (met Secret of JWK), niet in B2B-variant



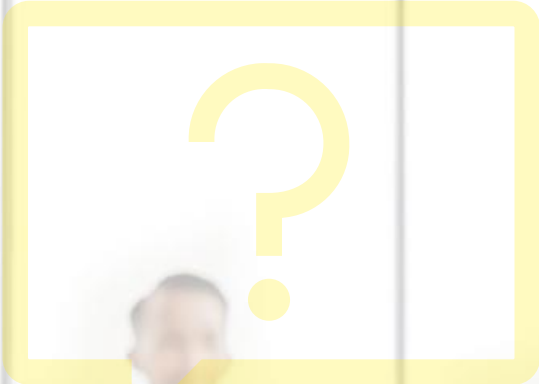
Wij contacteren u en bekijken de uitzonderingen **case per case**



Ik weet niet in welk scenario ik zit? Wat moet ik doen?



[Contacteer ons](#) en wij helpen u verder



Vragen?





**Demo ACM Selfservice Portaal
voor API-clients**

Structuur

Wat gaan we exact doen tijdens de demo?

- Over de scenario's heen: toegang geven tot het Selfservice Portaal via het Gebruikersbeheer (IDM)
- Scenario 1 en 2
 - Instellen van de permissies voor een Client
 - Instellen van een JWK voor een Client
 - Uitzondering: zelf een Client aanmaken voor je eigen organisatie
- Scenario 3 en 4
 - Een Client aanmaken namens een andere organisatie (use case van een dienstverlener)
 - Een delegatie voor een Client goedkeuren (klant van de dienstverlener)



Demo

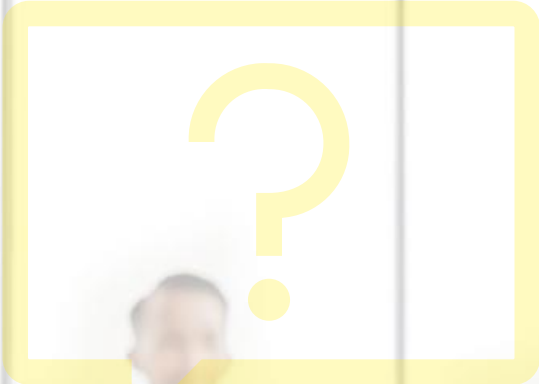
Links naar de verschillende toepassingen

Gebruikersbeheer van de Vlaamse overheid (IDM)

- T&I: <https://gebruikersbeheer-ti.vlaanderen.be>
- PRD: <https://gebruikersbeheer.vlaanderen.be>

ACM Selfservice Portaal

- T&I: <https://beheerportaal-ti.vlaanderen.be> (volledig operationeel vanaf start transitie)
- PRD: <https://beheerportaal.vlaanderen.be> (volledig operationeel vanaf start transitie)



Vragen?





Info en FAQ: Migratie van API-clients van Geosecure naar ACM
Stel uw vraag via onze mailbox uitfasinggeosecure@vlaanderen.be

Bedankt voor uw aandacht

uitfasinggeosecure@vlaanderen.be

**DIGITAAL
VLAANDEREN**



**Vlaamse
overheid**

