Modernisatie Certificatenbeheer: van Vo-DCB naar Vo-DCBaas

Infosessie 22/02/2021

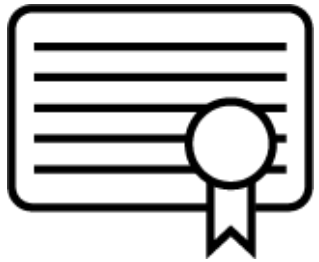
Sammy Roos (Digitaal Vlaanderen)
Frederik Gheys (Digitaal Vlaanderen)
Nathan Jacobs (Deloitte)

In deze infosessie

- **Inleiding bij het Certificatenbeheer**
  - → Wat is het Certificatenbeheer en waarom een modernisering?
  - → Toelichting bij het migratietraject en de roadmap
- **Toelichting bij de nieuwe DCBaaS-toepassing**
  - → Nieuwe concepten en rechtenmodel
  - → Een aantal eenvoudige voorbeelden en scenario's
- **Demo van de nieuwe DCBaaS-toepassing**
- **Q&A**

Vlaamse overheid

Wat is het Certificatenbeheer? (1)



Het Certificatenbeheer is een bouwsteen van de Vlaamse overheid waarmee je als organisatie (Vlaamse entiteit, lokaal bestuur, onderneming) zelf **certificaten kan aanvragen en beheren voor je toepassingen of API's**

- ✓ Beveiliging van het gegevensverkeer van en naar je toepassing of API
- ✓ X.509-certificaten die gratis worden uitgevaardigd door de Vlaamse certificatenautoriteit (bevestiging van de identiteit van diegene die het certificaat gebruikt)
- ✓ Gebruikt voor/door andere bouwstenen van de Vlaamse overheid (MAGDA, ACM/IDM, Geosecure, Datapower, enz.)

Vlaamse overheid

Wat is het Certificatenbeheer? (2)

- **Uit welke componenten bestaat het Certificaatbeheer?**

  → Vo-DCB: “Vlaamse overheid Digitaal Certificaten Beheer”
  - × Toepassing waarmee je certificaten kan aanvragen en beheren

  → Vo-PKI: “Vlaamse overheid Public Key Infrastructure”
  - × Achterliggende server infrastructuur waarmee de certificaten worden aangemaakt en ondertekend
    - → VOICA: “Vlaamse overheid Issuing Certificate Authority”
    - → VORCA: “Vlaamse overheid Root Certificate Authority”
  - × Controle van herroepen certificaten via CRL (“Certificate Revocation List”) en OCSP (“Online Certificate Status Protocol”)

Vlaamse overheid

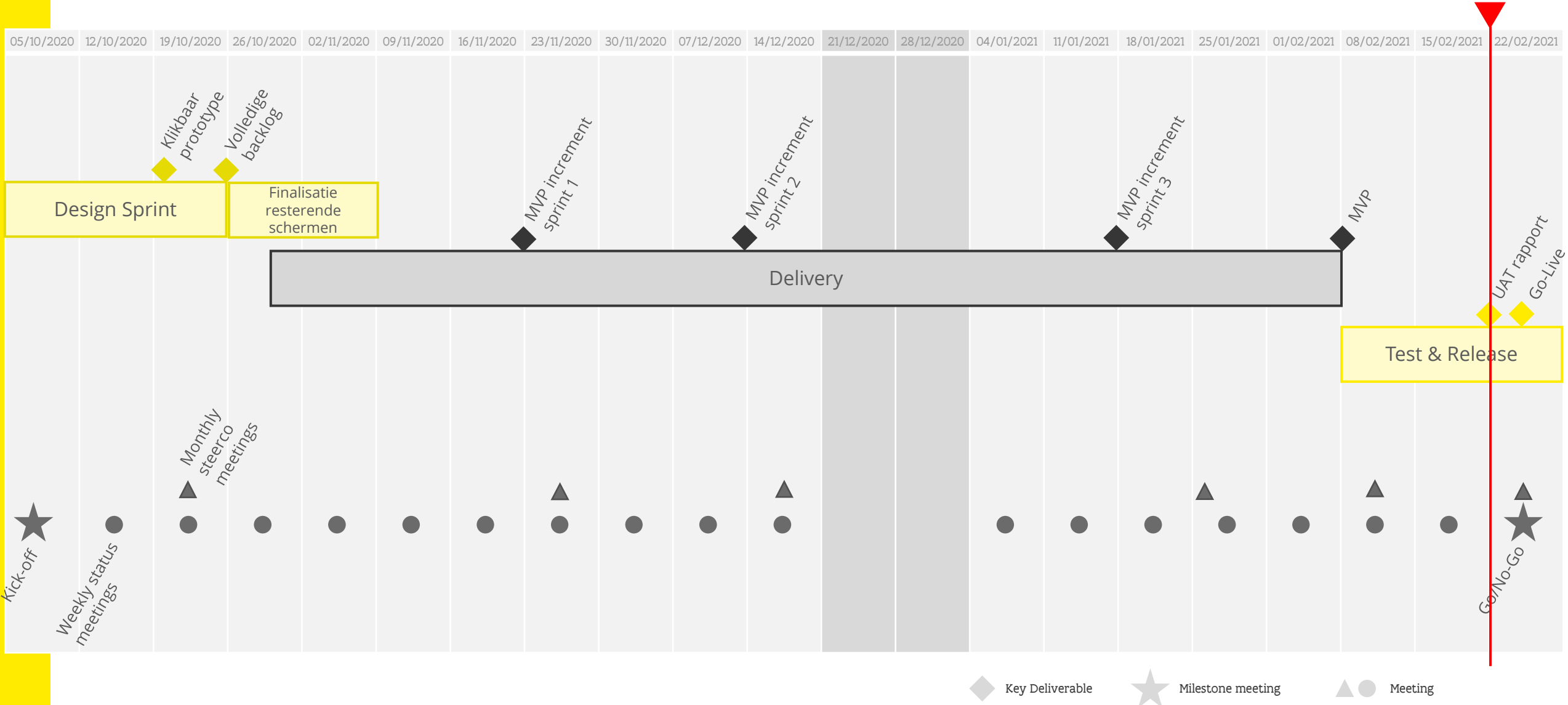
Keuze voor een volledige modernisering

- **Huidige Vo-DCB en haar achterliggende PKI-infrastructuur zijn verouderd**
  → Voldoen niet meer aan onze functionele vereisten
  → Voldoen niet meer aan onze veiligheidsvereisten

- **Keuze voor een nieuwe frontend-toepassing ("Vo-DCBaaS", Deloitte)**
  → Maximale selfservice: geen CN-aanvragen meer via e-mail
  → Nieuw rechtenmodel: ook certificaatbeheerder op niveau van organisatie

- **Keuze voor een nieuwe PKI-infrastructuur (via GlobalSign, Deloitte)**
  → Ondersteuning nieuwe cryptografische algoritmes (b.v. SHA3, EC)
  → In de toekomst: hoge volumes via API, automatisering via ACME
  → … maar nog steeds een private/interne PKI ! (scope blijft dezelfde)
  × Gebruik geen Vo-PKI-certificaten voor SSL/TLS-verkeer van een publieke website

Huidige planning



Migratie: sluiting NMC4 als katalysator

- **Huidige Vo-DCB en haar achterliggende PKI zijn gehost in NMC4-datacenter**
  → Deuren gaan onvoorwaardelijk dicht eind juni
  → Keuze om geen “lift & shift” te doen

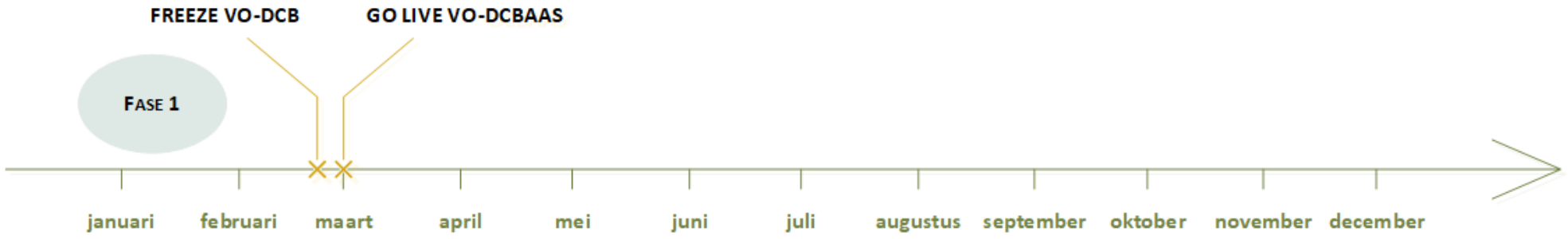
- **Versneld doorvoeren van de overschakeling naar Vo-DCBaaS en naar Vo-DCBaaS-certificaten in 2021**
  → Oude PKI-infrastructuur wordt stopgezet = nieuwe certificaten nodig

Vlaamse overheid

Migratie: overzicht

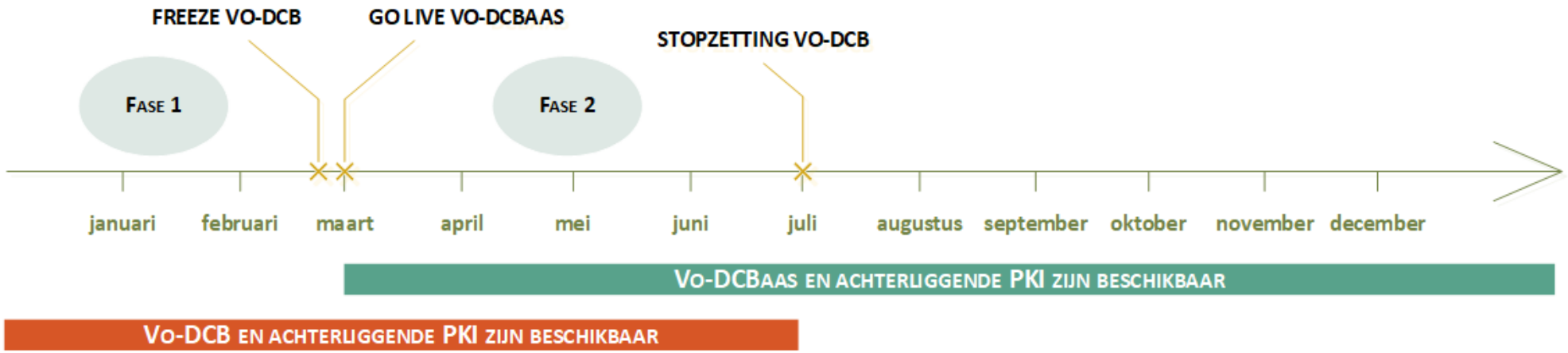
Vlaamse overheid

Migratie: overzicht



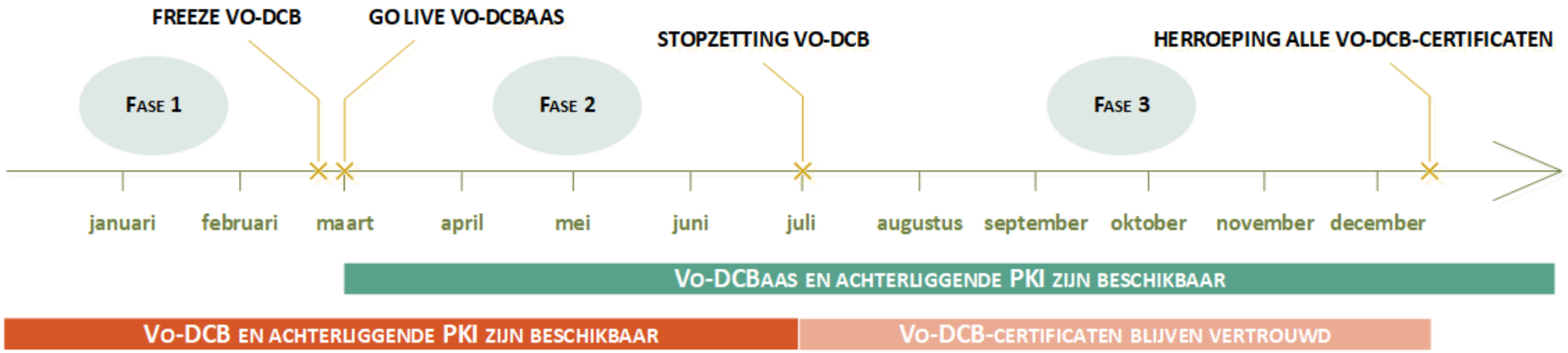
Vlaamse overheid

Migratie: overzicht



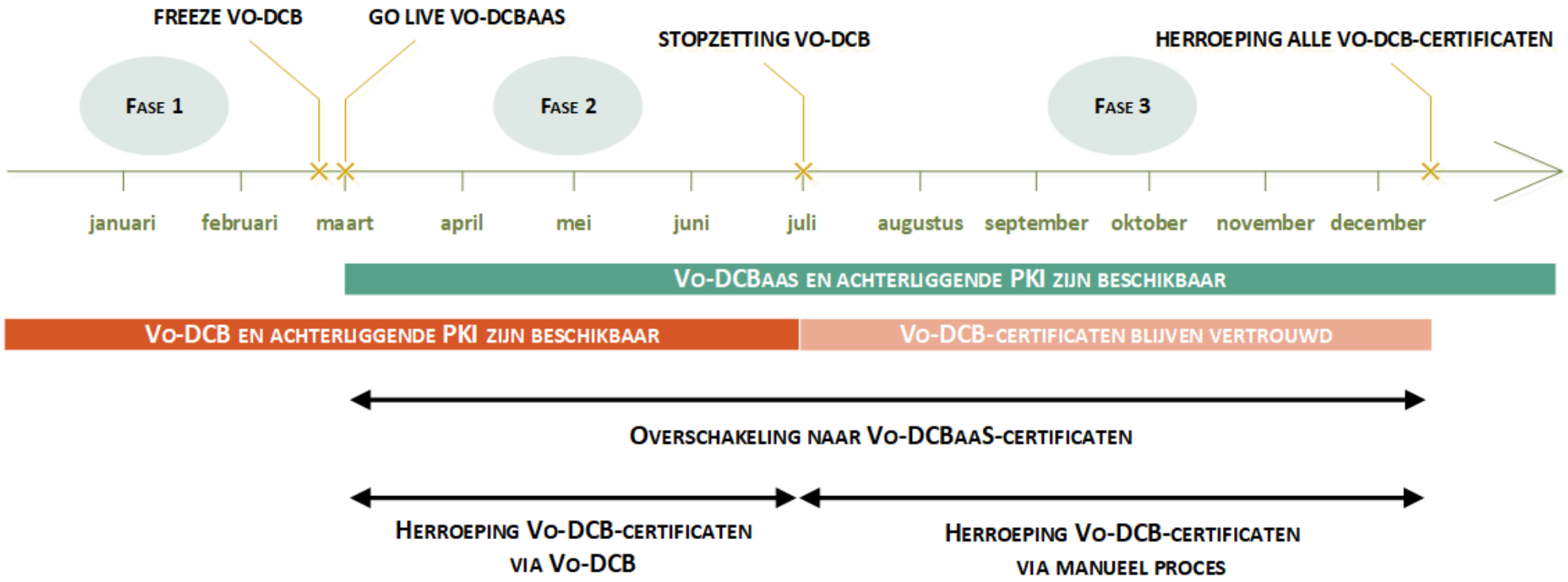
Vlaamse overheid

Migratie: overzicht



Vlaamse overheid

Migratie: overzicht



Vlaamse overheid

Fase 1: acties HFB/DV

Heden – 01/03/2021

Vo-DCBaaS is in ontwikkeling

Vo-DCB is beschikbaar

- **Verdere ontwikkeling en testing van Vo-DCBaaS**
  → Communicatie (direct/indirect), infosessies (22/02-26/02) en handleiding

- **22/02/2021: permanente "freeze" van Vo-DCB (!)**
  → Geen nieuwe CN's/certificaten, enkel beheer bestaande certificaten
  → Vanaf 01/03: nieuwe certificaten via Vo-DCBaaS
  → 22/02 - 01/03: geen enkele mogelijkheid om nieuwe certificaten aan te maken

- **Tussen 22/02 en 01/03: migratie van CN's naar Vo-DCBaaS**
  → Enkel de CN's worden gemigreerd, geen certificaten/CSR's/gebruikersrechten
  → Enkel de CN's met actieve certificaten (of vervallen in het laatste jaar)

Vlaamse overheid

Fase 1: acties klanten

Heden – 01/03/2021

Vo-DCBaaS is in ontwikkeling

Vo-DCB is beschikbaar

- **Proactief het gebruikersbeheer (IDM) in orde brengen**
  - → Nieuw rechtenmodel in DCBaaS: certificaatbeheer op verschillende niveaus
  - → Ken proactief al een “DCBaaS Certificaatbeheerder Organisatie” toe
  - → Andere rechten zijn beschikbaar bij Go Live DCBaaS

- **Proactief nieuwe root en intermediate certificaat installeren**
  - → Nieuwe PKI, dus VO-DCBaaS-certificaten hebben een nieuwe vertrouwensketen
  - → Zijn al beschikbaar op https://documenten-pki.vlaanderen.be/

Vlaamse overheid

Fase 2: acties HFB/DV

01/03/2021 – 30/06/2021

Vo-DCBaaS is beschikbaar

Vo-DCB is beschikbaar

- **Go Live Vo-DCBaaS en achterliggende PKI op 01/03/2021**
  - → Vo-DCBaas = bron om nieuwe certificaten aan te vragen
  - → Vo-DCBaaS-certificaten hebben een andere vertrouwensketen
  - → Nieuwe CRL voor Vo-DCBaaS-certificaten

- **Vo-DCB blijft in deze fase nog bestaan**
  - → Vo-DCB = bron om enkel bestaande Vo-DCB-certificaten te beheren
  - → Vo-DCB-certificaten blijven in deze fase vertrouwd
  - → CRL wordt nog steeds geactualiseerd en blijft beschikbaar

Vlaamse overheid

Fase 2: acties klanten

01/03/2021 – 30/06/2021

Vo-DCBaaS is beschikbaar

Vo-DCB is beschikbaar

- **Vervangen van oude Vo-DCB-certificaten door nieuwe Vo-DCBaaS-certificaten**
  - → Aanbevolen, niet verplicht
    - × Vo-DCB-certificaten zullen ook nog in de volgende fase vertrouwd blijven (zie verder), maar het beheren ervan wordt moeilijker door wegvallen van de Vo-DCB-toepassing na 30/06/2021
  - → Vergeet vervangen certificaten niet te herroepen in Vo-DCB
  - → Kosten voor certificatenwissel: specifieke optie in AMaaS
    - × Overleg met HB-Plus is ongoing hoe we klanten best kunnen begeleiden
  - → Niet te vergeten: stappen van fase 1
    - × Toegang verlenen tot de DCBaaS-toepassing
    - × Nieuwe root en intermediate certificaat installeren

Vlaamse overheid

Fase 3: acties HFB/DV

01/07/2021 – 15/12/2021

Vo-DCBaaS is beschikbaar

Vo-DCB is stopgezet

- **Stopzetting Vo-DCB en achterliggende PKI op 30/06/2021**
  - → Exacte datum onder voorbehoud, nog verder te communiceren
  - → Toepassing niet meer bereikbaar, geen meldingen van te vervallen certificaten of beheer van oude certificaten meer
- **… maar Vo-DCB-certificaten blijven nog vertrouwd tot 15/12/2021**
  - → Creatie van een manueel proces met HB-Plus om revocaties mogelijk te maken
    - × Digitaal Vlaanderen draagt de kosten van deze manuele revocaties (verschil met vorige communicaties)
  - → CRL van Vo-DCB wordt geactualiseerd en blijft beschikbaar (manueel proces)
  - → We communiceren nog over de concrete werkwijze
- **Op 15/12/2021 gaan wij alle Vo-DCB-certificaten herroepen**
  - → Root en intermediate certificaat oude PKI-infrastructuur worden herroepen

Fase 3: acties klanten

01/07/2021 – 15/12/2021

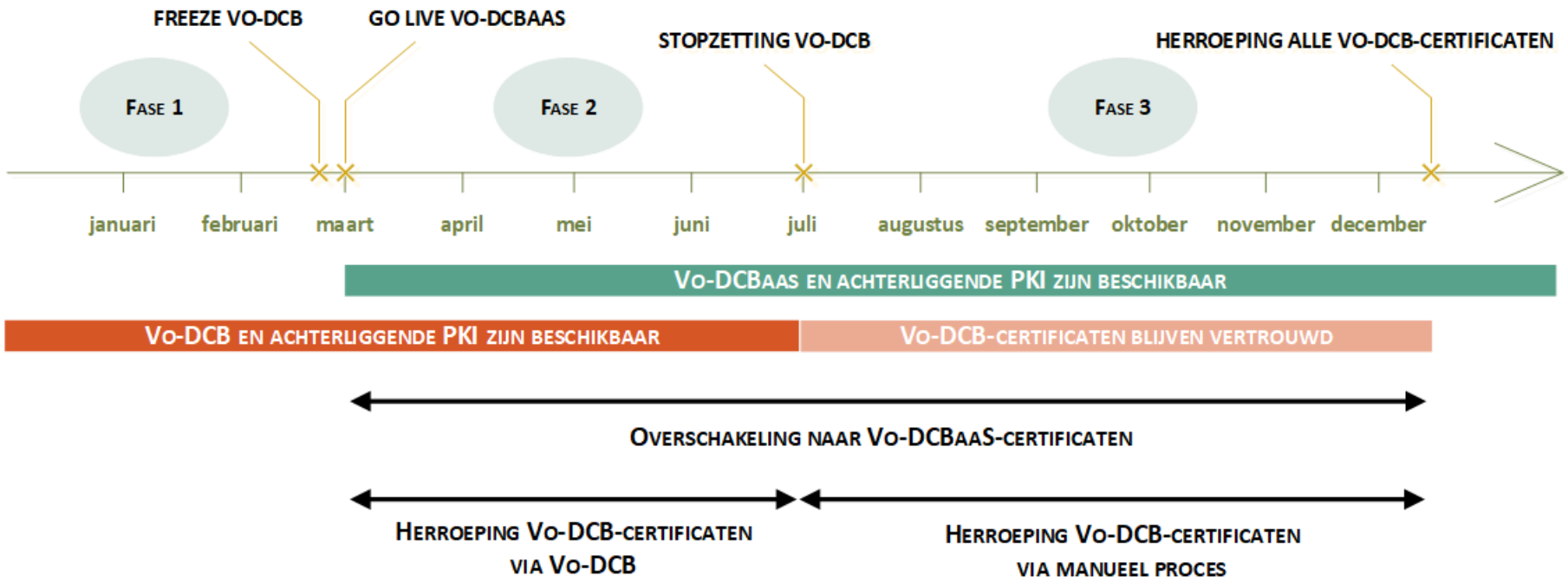
Vo-DCBaaS is beschikbaar

Vo-DCB is stopgezet

- **Vervangen van oude Vo-DCB-certificaten door nieuwe Vo-DCBaaS-certificaten**
  - → In deze fase verplicht, deadline is 15/12/2021
    - × Na 15/12/2021 verliezen certificaten hun vertrouwensketen (root en intermediate certificaat zijn niet meer vertrouwd)
  - → Vergeet vervangen certificaten niet te herroepen via manuele procedure
  - → Kosten voor certificatenwissel: specifieke optie in AMaaS
    - × Overleg met HB-Plus is ongoing hoe we klanten best kunnen begeleiden
  - → Niet te vergeten: stappen van fase 1
    - × Toegang verlenen tot de DCBaaS-toepassing
    - × Nieuwe root en intermediate certificaat installeren

Vlaamse overheid

Migratie: korte samenvatting



Vlaamse overheid

Roadmap voor Vo-DCBaaS

- **Release van 01/03: MVP van het Certificatenbeheer**
  - → Starten met de basisfunctionaliteiten
- **Snel een aantal nieuwe releases voor extra functionaliteit**
  - → Backlog met een aantal functionaliteiten die zijn uitgesteld in MVP
    - × Aanvragen van toepassingen voor een andere organisatie (dienstverleners!)
    - × Extra functionaliteit rond het valideren van certificaten
- **Q2-Q3: fase 2 met functionele uitbreidingen om selfservice te verhogen**
  - → VRD2: API-ondersteuning voor Vo-DCBaaS (MAGDA)
  - → Behoeften? Laat het ons weten!

Vlaamse overheid

In deze infosessie

- **Inleiding bij het Certificatenbeheer**
  - → Wat is het Certificatenbeheer en waarom een modernisering?
  - → Toelichting bij het migratietraject en de roadmap
- **Toelichting bij de nieuwe DCBaaS-toepassing**
  - → Nieuwe concepten en rechtenmodel
  - → Een aantal eenvoudige voorbeelden en scenario's
- **Demo van de nieuwe DCBaaS-toepassing**
- **Q&A**

Vlaamse overheid

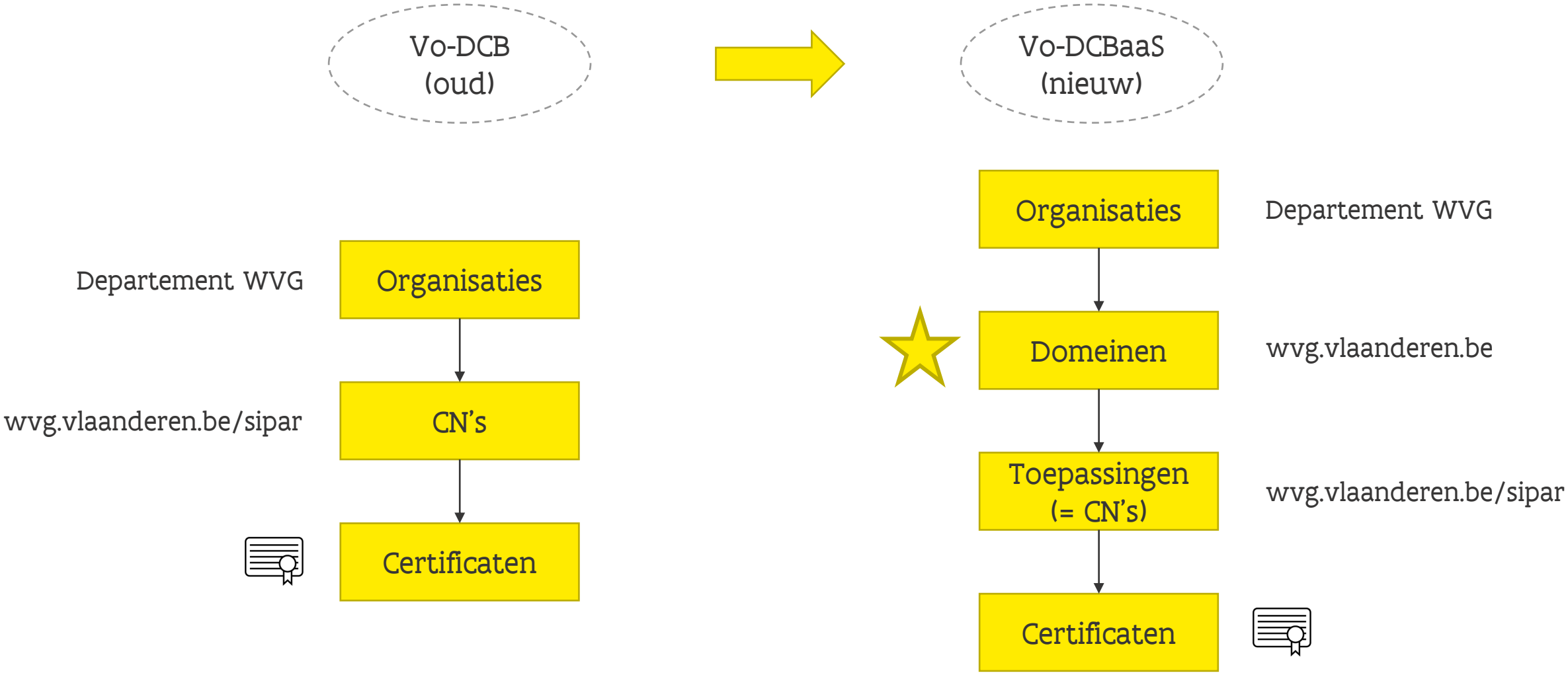
Centrale principes van Vo-DCBaaS

- **Selfservice voor organisaties (kortere doorlooptijd, onafhankelijk van centrale processen, maximale autonomie bij klanten)**
  - → Aanvragen gebeuren allemaal in de toepassing zelf (workflows)
    - × Zoveel mogelijk automatische goedkeuring van nieuwe CN's
    - × Zo weinig mogelijk tussenkomst van DCBaaS-beheerders

- **Ondersteunen van verschillende gebruikersscenario's**
  - → Aanvragen van CN's voor eigen organisatie (bestaand)
  - → Aanvragen van CN's in naam van andere organisatie (nieuw)
    - × Handig voor dienstverleners

Vlaamse overheid

Nieuwe concepten in Vo-DCBaaS (MVP)(1)



Nieuwe concepten in Vo-DCBaaS (MVP)(2)

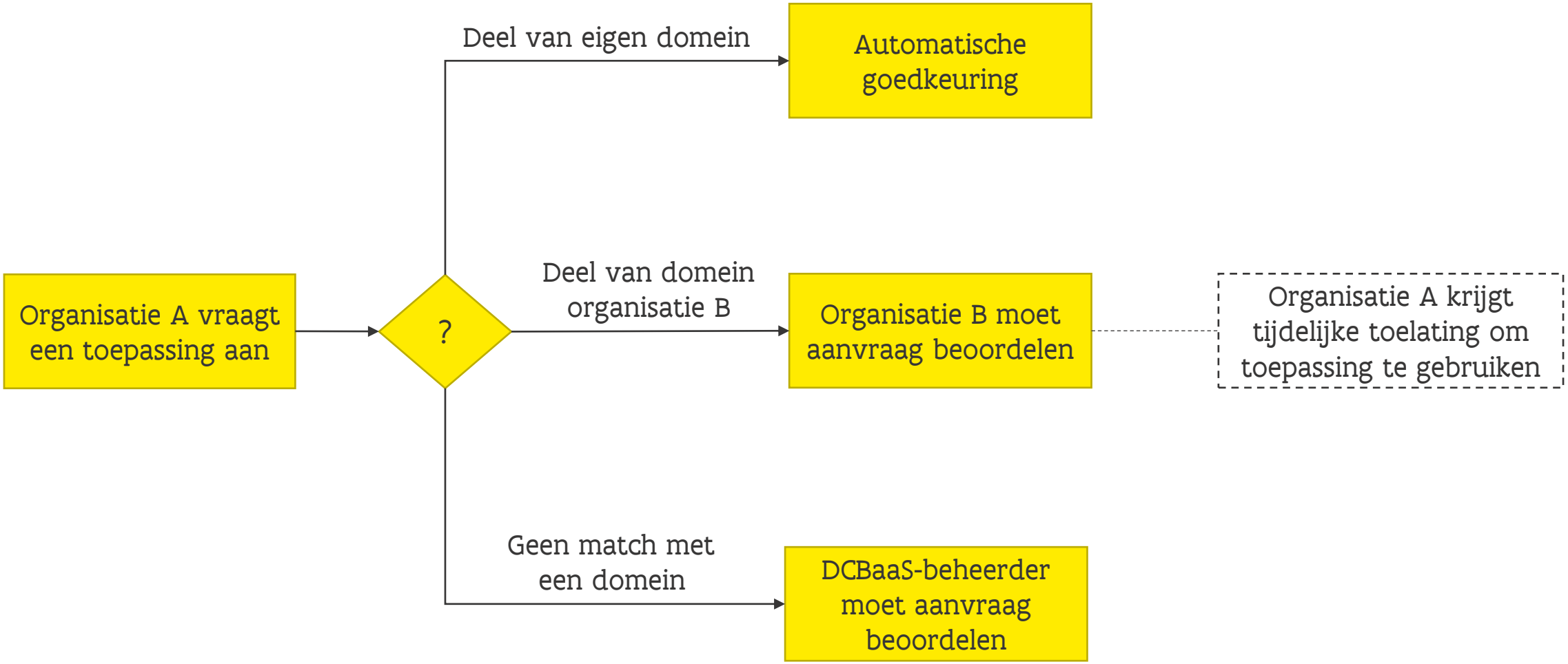
- **“Domein” als nieuw niveau tussen organisaties en toepassingen (CN’s)**

  → Mechanisme om organisaties zelf regels te laten opleggen voor bepaalde groepen van toepassingen
  - × Bepalen welke types certificaten mogen aangemaakt worden

  → Mechanisme om nieuwe toepassingen (CN’s) automatisch te laten goedkeuren of organisaties zelf te laten beslissen over goedkeuring
  - × Verschillende scenario’s mogelijk (zie volgende slide)

  → Domeinen worden aangevraagd door de organisaties zelf, maar goedgekeurd door de DCBaaS-beheerders

Nieuwe concepten in Vo-DCBaaS (MVP)(3)



Extra aanvullingen na de MVP

- **Nog geen onderdeel van de MVP, maar worden toegevoegd in de komende weken**

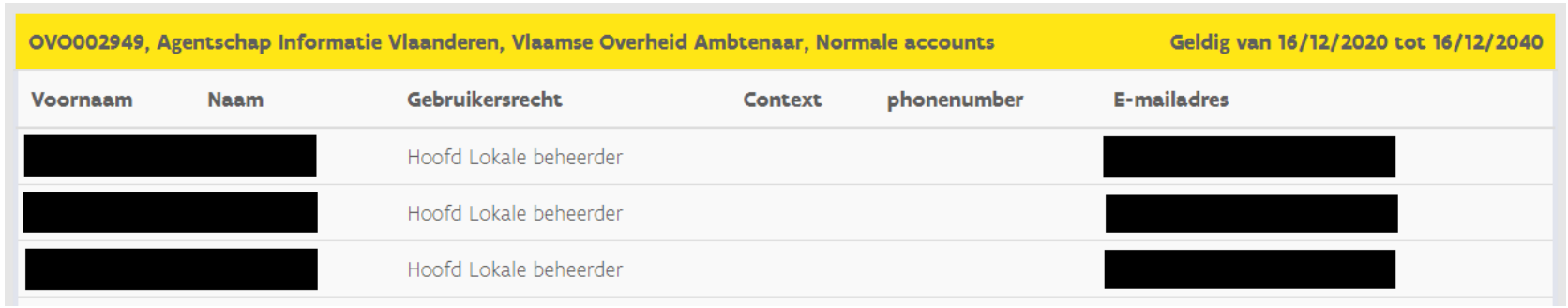
  → Aanvragen namens andere organisaties (validatieregels)
  → SAN validatie
  → Algemene “quality of life”-verbeteringen

  Feedback welkom uiteraard!

Vlaamse overheid

Nieuwe rechtenmodel (1)

- **Rechten voor Vo-DCBaaS kunnen toegekend worden door lokale beheerders in het Gebruikersbeheer van de Vlaamse overheid (IDM)**
  - → Hoe weet ik wie mijn lokale beheerder is?
    - × https://mijnprofiel-gebruikersbeheer.vlaanderen.be
    - × Klik op “Mijn Lokale beheerders”



OVO002949, Agentschap Informatie Vlaanderen, Vlaamse Overheid Ambtenaar, Normale accounts — **Geldig van 16/12/2020 tot 16/12/2040**

Voornaam	Naam	Gebruikersrecht	Context	phonenumber	E-mailadres
[redacted]		Hoofd Lokale beheerder			[redacted]
[redacted]		Hoofd Lokale beheerder			[redacted]
[redacted]		Hoofd Lokale beheerder			[redacted]

  - → Rechten van de oude DCB-toepassing worden niet gekopieerd!

Vlaamse overheid

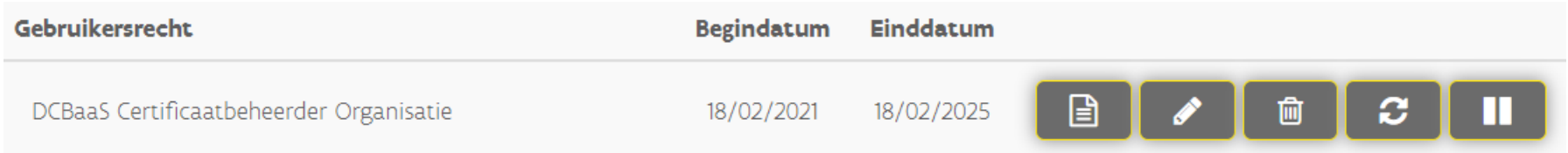
Nieuwe rechtenmodel (2)

- Volgende rollen zijn beschikbaar voor alle organisaties
  - → **DCBaaS Certificaatbeheerder Organisatie (nieuw)**
    - × Leesrechten op alle objecten binnen de organisatie
    - × Kan toepassingen aanvragen en certificaten aanmaken (voor alle toepassingen binnen de organisatie)
  - → **DCBaaS Certificaatbeheerder Toepassing (bestond al in Vo-DCB)**
    - × Leesrechten op alle objecten binnen de organisatie
    - × Kan certificaten aanmaken (voor alle toepassingen waarop de gebruiker recht heeft)
  - → **DCBaaS Workflowbeheerder (nieuw)**
    - × Leesrechten op domeinen, toepassingen en aanvragen van de organisatie
    - × Kan toepassingen aanvragen en toepassingsaanvragen (door andere organisaties) op de eigen domeinen goedkeuren/afkeuren
    - × Kan domeinen aanvragen

Nieuwe rechtenmodel (3)

- **DCBaaS-beheerdersrechten zijn enkel beschikbaar voor Digitaal Vlaanderen**
  → Functiescheiding tussen algemene applicatiebeheerder en persoon die de configuratie van de toepassing kan instellen

- **Nieuwe rechten zullen beschikbaar zijn vanaf 01/03 in Gebruikersbeheer**
  → … maar “DCBaaS Certificatenbeheerder Organisatie” is nu al beschikbaar om snelle opstart mogelijk te maken!



Vlaamse overheid

Samenwerking met dienstverlener? (1)

- **Veel entiteiten werken samen met een ICT-dienstverlener**
  - → Maken vaak op de achtergrond de certificaten in orde
  - → Omslachtig in de oude toepassing: Entiteit moet zelf nog bepaalde acties doen, pingpong tussen de verschillende partijen

- **Nieuwe model van Vo-DCBaaS geeft daar veel meer flexibiliteit**
  - → Een aantal scenario's mogelijk
  - → Kernvraag is in welke mate je zelf nog controle wil blijven behouden over je sleutels en zelf de certificaten wil aanvragen

Vlaamse overheid

Samenwerking met dienstverlener? (2)

- **Scenario 1: volledig eigen beheer**
  → Entiteit doet zelf alle aanvragen in Vo-DCBaaS (aanvragen toepassing, aanvragen certificaat) en geeft door aan dienstverlener (zoals vroeger in Vo-DCB)

- **Scenario 2: mix van eigen beheer + uitbesteden (nog niet mogelijk in MVP)**
  → Dienstverlener doet de aanvraag van de toepassing (b.v. wvg.vlaanderen.be/sipar) in naam van zijn klant, maar de entiteit vraagt zelf nog het certificaat aan en geeft door

- **Scenario 3: volledig uitbesteden aan dienstverlener**
  → Dienstverlener vraagt de toepassing (b.v. wvg.vlaanderen.be/sipar) aan op haar eigen organisatie (b.v. HB+)
  → Entiteit keurt de toepassingsaanvraag (op haar domein) goed in Vo-DCBaaS
  → Dienstverlener kan zelf het certificaat aanvragen, zonder tussenkomst entiteit

Technische specificaties voor de CSR (MVP)

- **Maximale autonomie en flexibiliteit voorzien via templating functionaliteit**
- **Ondersteunde algoritmes: RSA**
  → SHA-256, SHA-384, SHA-512
- **Ondersteunde sleutellengtes**
  → 2048 en 4096 (aanbevolen)
- **Maximale duurtijd van het certificaat: 24 maanden**
- **Common name, country (“BE”) en organization zijn verplicht**
  → Alle andere velden zijn optioneel
- **Mogelijkheid om tot 100 SAN’s in te vullen**
  → DNS, e-mails, IP-adressen, URI’s

Vlaamse overheid

In deze infosessie

- **Inleiding bij het Certificatenbeheer**
  - → Wat is het Certificatenbeheer en waarom een modernisering?
  - → Toelichting bij het migratietraject en de roadmap
- **Toelichting bij de nieuwe DCBaaS-toepassing**
  - → Nieuwe concepten en rechtenmodel
  - → Een aantal eenvoudige voorbeelden en scenario's
- **Demo van de nieuwe DCBaaS-toepassing**
- **Q&A**

Vlaamse overheid

Demo van de nieuwe DCBaaS-toepassing (1)

- **Een aantal eenvoudige voorbeelden en scenario's**

  → Aanmelden en algemene look & feel van de toepassing

  → Creëren van een certificaat onder een bestaande toepassing
  - × Downloaden van het certificaat
  - × Herroepen en verwijderen van het certificaat

  → Aanvragen van een nieuwe toepassing
  - × Deel van eigen domein
  - × Deel van domein van andere organisatie

  → Aanvragen van een domein

Demo van de nieuwe DCBaaS-toepassing (2)

T&I: https://dcb-ti.vlaanderen.be

PRD: https://dcb.vlaanderen.be
(nog niet actief)

Vlaamse overheid

In deze infosessie

- **Inleiding bij het Certificatenbeheer**
  - → Wat is het Certificatenbeheer en waarom een modernisering?
  - → Toelichting bij het migratietraject en de roadmap
- **Toelichting bij de nieuwe DCBaaS-toepassing**
  - → Nieuwe concepten en rechtenmodel
  - → Een aantal eenvoudige voorbeelden en scenario's
- **Demo van de nieuwe DCBaaS-toepassing**
- **Q&A**

Vlaamse overheid

Q&A

- **Later nog vragen?**
  → Contacteer ons via vodcb@vlaanderen.be
- **Bekijk onze toelichtingen en FAQ's op onze website**
  → Worden doorheen het project aangevuld, zie het luikje "Vo-DCB/Vo-DCBaaS"
- **Blijf op de hoogte van update via de ICT-nieuwsbrief van Digitaal Vlaanderen**
  → Inschrijven via deze link

Vlaamse overheid