NOTIFICATIE MANAGEMENT COMPONENT

De nieuwe kern van de NMC

Nooit een notificatie verloren, altijd een eindstatus die de dienstverlener kan zien

de reis van een notificatie | één bron van waarheid | werk als rijen | als het misgaat | de dienstverlener | privacy

Van buiten hetzelfde, van binnen een ander mechanisme

1

Er gaat niets meer verloren

Aangenomen zodra ze in onze database staat. Elke notificatie zonder eindstatus heeft altijd een open taak.

2

Niet meer afhankelijk van de callback van NotifyNL

Die komt uiterlijk vijf keer en is dan weg. Nu slaan we receipts eerst op, vragen zelf na als dat nodig is, en stellen bezorging pas na zeven dagen vast.

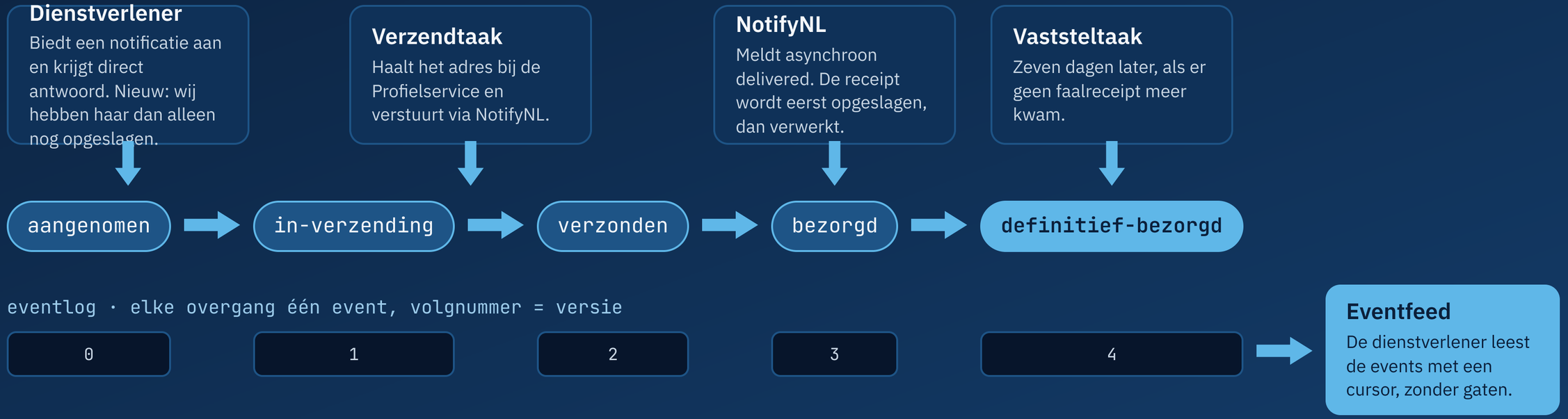
3

Een afleverbewijs waar de dienstverlener op kan bouwen

Een eventlog met elke statuswijziging, dat hij zelf kan uitlezen.

> Hiervoor stuurde de NMC notificaties. Nu nog steeds. Het verschil zit in wat er gebeurt als het misgaat.

Van aanname tot definitief bezorgd



Elke stap na de aanname is een taak in de database met een tijdstip waarop ze aan de beurt is. De dienstverlener wacht nergens op.

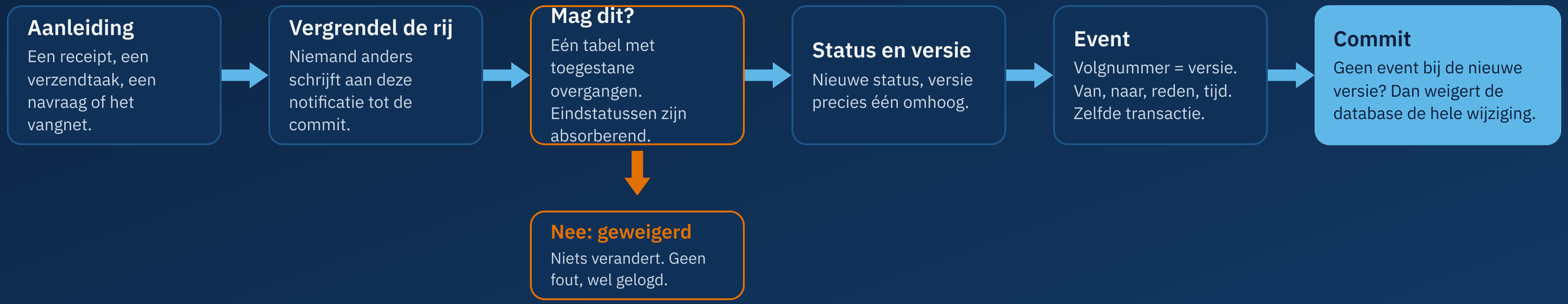
> Antwoord zodra de notificatie bij ons is opgeslagen. Daarna doet de NMC het werk, en legt elke stap vast als event.

Vier dingen die vroeger stil bleven liggen

NotifyNL of de Profielservice is onbereikbaar	De taak wordt uitgesteld en later opnieuw geprobeerd.	**Verzonden zodra het weer kan.** De notificatie gaat niet verloren.
De receipt blijft uit: niet ontvangen van NotifyNL	De NMC vraagt het periodiek zelf na bij NotifyNL.	De uitkomst alsnog. Blijft die uit, dan **bezorgstatus-onbekend**.
Een pod valt uit midden in het verzenden	Een andere pod claimt de taak en vraagt NotifyNL eerst of de e-mail al is aangeboden.	**Geen dubbele e-mail**, geen verloren notificatie.
Receipts botsen: twee tegelijk, of één vóór onze eigen commit	Eerst opslaan, dan verwerken onder de rijvergrendeling, in de volgorde van het tijdstip in de receipt.	Een **oudere of dubbele receipt verandert niets**. Niets wordt overschreven.

> Elke notificatie zonder eindstatus heeft een open taak of een timer. Niets blijft stil liggen.

Hoe een status verandert



PostgreSQL · vier tabellen, geen broker, geen workflow-engine

notificatie
De huidige status en versie. Wat de dienstverlener te zien krijgt.

verzending
Elke aflevering via NotifyNL apart, met de letterlijke uitkomst.

event
Het afleverbewijs: alleen toevoegen, nooit wijzigen.

taak
Al het werk en alle timers, als rijen.

> Eén functie schrijft de status. Werk, overgang en event committen samen, of helemaal niet.

De takentabel en de pods

Takentabel

verzenden	nu
receipt verwerken	nu
navraag	over 1 uur
vaststellen	over 7 dagen
wissen	over 14 dagen

Elke bijwerking is een rij; een timer is een tijdstip.

Claim: elke pod pakt wat aan de beurt is en niet al door een ander wordt vastgehouden.

pod 1 20 taken, 2 min lease

pod 2 20 taken, 2 min lease

pod 3 slaat bezette rijen over

Uitvoeren

De aanroep naar NotifyNL of de Profielservice valt buiten elke databasetransactie.

Binnen het verzendbudget: 1400 per minuut, eerlijk verdeeld over dienstverleners.

Afronden

Alleen als de claim nog van deze pod is. Heeft een ander de taak inmiddels, dan rolt alles terug.

Een fout betekent opnieuw proberen met oplopende wachttijd; na vijf keer wacht de taak op beheer.

vangnet · elke 5 minuten

Controletaak

Zoekt elke notificatie zonder eindstatus en zonder open taak, en plant de taak die bij haar status hoort. Kan niets haar verder brengen, dan krijgt ze alsnog een eindstatus.

> Pods verdelen het werk zonder coördinatie. Een piek buffert als rijen en loopt gelijkmatig weg.

Twee wegen uit hetzelfde eventlog

eventlog

Elke overgang één event

Volgnummer, van, naar, reden, tijd. Geen e-mailadres, geen BSN, geen referentie van de dienstverlener.

altijd

Eventfeed met cursor

De dienstverlener haalt de events op in volgorde, zonder gaten, en bevestigt zelf tot waar hij is. Werkt voor iedereen, ook zonder inkomend endpoint.

optioneel

Webhook

Dezelfde events, ondertekend, in bundels van 100. Bij fouten wacht en pauzeert hij vanzelf. Een 2xx is geen bevestiging.

Dienstverlener

Herkent hetzelfde event in beide wegen aan dezelfde id.

Ziet aan het volgnummer per notificatie of een update is ingehaald.

Kent tien statussen, met een reden bij een eindstatus: onbereikbaar, geen contactgegevens, technisch, verlopen, geannuleerd.

⚠ **Wat verandert voor de dienstverlener:** de aanname antwoordt 202 in plaats van 200 · eigen statuswaarden in plaats van die van NotifyNL · de callback-URL per notificatie vervalt, de webhook staat per dienstverlener in het register.

De feed geeft zekerheid, de webhook geeft snelheid. Bevestigen doet de dienstverlener zelf.

Persoonsgegevens: zo kort als het kan

aanname

Versleuteld op de rij

Ontvanger en inhoud, met een eigen sleutel per notificatie.

verzenden

Alleen de verzendtaak leest

Geen endpoint, log of event bevat de klare tekst. Beheer heeft geen leespad.

eindstatus

Bezorgd, of niet

Vanaf hier lopen de termijnen.

+ 7 dagen

Sleutel gewist

De gegevens zijn niet meer te openen. De rij is pseudoniem, het afleverbewijs blijft.

+ 365 dagen

Rij weg

Met alles wat erbij hoort. Het eventlog wordt per partitie opgeruimd.

Het eventlog was nooit persoonlijk

Alleen id's, statussen, redenen en tijdstippen. Het mag daarom een jaar blijven als afleverbewijs.

Sleutelrotatie zonder herversleutelen

Elke notificatiesleutel is op zijn beurt versleuteld met een hoofdsleutel. Roteren raakt alleen die laag.

Het adres wordt nooit bewaard

Bij centrale regie komt het e-mailadres uit de Profielservice, wordt gebruikt en niet opgeslagen.

> Nooit een notificatie verloren, altijd een eindstatus, en zeven dagen later geen persoonsgegevens meer.