



Technisch ontwerp

Brabantse Zorgvuldigheidsscore Veehouders
(BZV)

Opdrachtgever:
Project:
Versie:
Datum:

Provincie Noord Brabant
Brabantse Zorgvuldigheidsscore Veehouders (BZV)
0.3
9-2-2023

DOCUMENTHISTORIE

Versiebeheer

Versie	Datum	Auteur	Samenvatting van de wijzigingen
0.1			Initieel document
0.2			Initieel document; aangevuld na overleg PNB
1.0			Aangevuld na controle PNB; entiteiten aangevuld.

Distributie

Versie	Datum	Naam	Organisatie	Functie
1.0			PNB	BZV Beheer
1.0			PNB	BZV Beheer

Inhoud

1	Introductie	4
2	Infrastructuur	5
2.1	Client omgeving	5
2.2	Windows Server 2019	6
2.2.1	SQL Server	6
2.2.2	IIS	6
2.2.3	MailServer	6
2.2.4	Azure DevOps Agent	6
3	Software	7
3.1	BZV-website	7
3.1.1	Doel	7
3.1.2	Gebruikte componenten	7
3.1.3	Indeling oplossing (.sln)	7
4	Taken	8
5	Website eHerkenning	9
5.1	Doel	9
5.2	Gebruikte componenten	9
6	Website BZV	10
6.1	Gebruikers	10
7	Scenario's	12
7.1	Modules/maatlaten	13
7.2	Kengetallen	14
7.3	Domeinen	14
8	Parameters	15
9	Navigatie	15
10	Rekenmodule	16
11	Certificaten	18
12	eHerkenning	18
12.1	Dienstverlener inrichting	19
12.2	Nieuwe Signicat certificaten	21
12.3	Nieuw eHerkenningcertificaat WebServer	21
13	Database entiteiten model	23
13.1	Kengetallen, modules en domeinen	23
13.2	Certificaatinrichting	24
13.3	Scenario inrichting	25

13.3.1	Scenario status / fiatting status.....	26
13.3.2	Scenario Stallen	27
13.4	Diersoorten.....	28
13.5	Configuratie maatlatten (parameters)	29
13.6	Versies	29
13.7	Menu, legenda en sidepanels.....	30
13.8	Gebruikers	31
13.9	Aanmeldingen.....	32
13.10	Vergelijkingsrapportage.....	33
13.11	Rapportage tabellen	33

1 INTRODUCTIE

De Brabantse Zorgvuldigheidsscore Veehouderij (BZV) is een systeem waarmee de Provincie Noord-Brabant ondersteund wordt in de bepaling of een bedrijf (veehouder) zorgvuldig is en als zodanig in aanmerking komt vooruitbreiding.

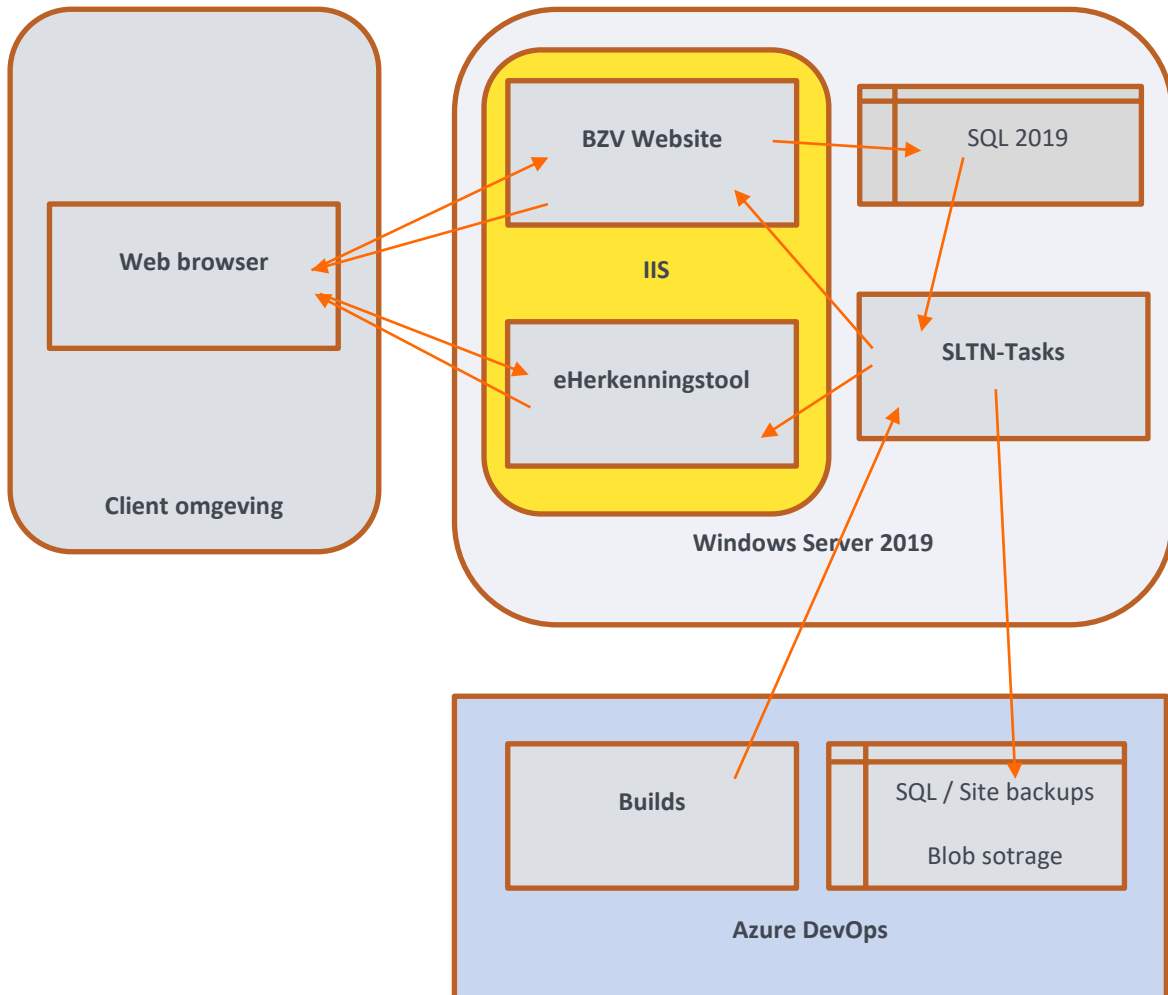
De berekening van de BZV-score vindt plaats door een webapplicatie genaamd BZV. Dit document beschrijft het technisch ontwerp van deze applicatie.

In dit document wordt soms verwezen naar een versie. Dit is de applicatie versie of de BZV-configuratie versie en deze verschillen. De BZV-configuratie versie wordt beheerd door de provincie Noord-Brabant. De applicatie versie door het ontwikkelteam.

Niet alle C# en T-SQL-code wordt beschreven; De code is beschrijvend. De database is ook opgenomen als .sql bestanden in de C# oplossing.

2 INFRASTRUCTUUR

Hieronder staat een overzicht van de componenten die betrokken zijn bij de BZV-applicatie:



Het geheel is niet lastiger dan het is. De acceptatie-omgeving en productie-omgeving kunnen theoretisch bij elkaar op 1 server. Dit is niet aan te raden omdat door fouten in de C# code, configuratie of T-SQL in theorie de verkeerde database benaderd zou kunnen worden.

2.1 Client omgeving

De BZV Website is gemaakt voor de volgende browsers:

- Firefox
- Edge
- Chrome

De website is een client-server applicatie met html en javascript. Mobiele apparaten worden met uitzondering van de startpagina en het publieke gedeelte niet ondersteund.

2.2 Windows Server 2019

De omgeving waar de website op draait is een Windows Server 2019. Hierop draaien de volgende onderdelen:

- SQL Server 2019 + back-up-agent
- IIS (Internet Information Services)
- Azure DevOps Agent

Oudere versies dan Windows 2019 Server worden vanwege de Connectis eHerkenning niet ondersteund.

2.2.1 SQL Server

Dit is een standaard editie van SQL-Server 2019. Back-ups worden gemaakt door de hosting-partij en vallen buiten scope van dit document.

Binnen SQL-Server worden alleen standaard functionaliteiten gebruikt. Er zijn geen C# (of andere talen) bibliotheken geïmporteerd op de server.

De SQL-server gebruikt voor de toegang tot de database SQL-gebruikers (SltnBZV) die bijna alles mogen op de server. De gebruiker is een db-owner. Er wordt geen gebruik gemaakt van geïntegreerde beveiliging, maar dat is wel instelbaar.

2.2.2 IIS

Er wordt gebruik gemaakt van de laatste versie van IIS die beschikbaar is op Windows Server 2019. De websites BZV en eHerkenningstool kunnen beiden dezelfde application pool gebruiken, maar dat is niet noodzakelijk. De eHerkenningstool staat normaliter uit en heeft geen impact op de normale werking.

De website application identity moet (lees+executie+schrijf) rechten hebben op de website folder en op de eHerkenningconfiguratie folder.

2.2.3 MailServer

Er is een mailserver geïnstalleerd waarmee email kan worden verstuurd. Deze mailserver maakt gebruik van het SMTP-protocol. Er wordt alleen mail verstuurd, niet binnengehaald. Het beheer van deze server valt buiten de scope van dit document.

2.2.4 Azure DevOps Agent

De Azure DevOps Agent wordt gebruikt om releases te plaatsen. De Windows 2019 omgeving is niet toegankelijk voor de software-ontwikkelaars. Opleveringen, database-aanpassingen, database-queries en database-backups benodigd voor ontwikkelaars gaan via een Azure DevOps agent. Een speciale tool, genaamd SLTN-Tasks kan gespecialiseerde taken uitvoeren.

Deze DevOps Agent zorgt ook voor een veilige OTAP-distributie over de omgevingen

3 SOFTWARE

De code voor de gehele BZV-applicatie is verdeeld over 2 Visual Studio C# oplossingen (.sln). De website is gemaakt in C# ASP .Net MVC voor .NET Framework 4.8 met behulp van Razor Pages. Deze .NET versie wordt nog een aantal jaar ondersteund (op Windows 2019); maar moet wel binnen een paar jaar omgezet worden naar een .NET (Core) versie 7 of hoger.

Voor het beheer van de website op de acceptatie- en productie-server is er ook een C# oplossing, maar deze is geschreven in .NET Core 7.0. Deze applicatie is gemaakt voor systeembeheer doeleinden, tbv. Release deployment en backups. Deze solution is buiten scope van dit document omdat deze volledig gericht is op het beheer door SLTN.

Hoe de oplossingen zijn ingericht, met de bijbehorende folders-structuur wordt niet beschreven in dit document. Er zijn maar 2 oplossingsfolders en de folderstructuur wijst zich vanzelf.

3.1 BZV-website

3.1.1 Doel

De website kent publieke- en eindgebruikers. Publieke gebruikers hebben een klein gedeelte van de website ter beschikking. Eindgebruikers moeten inloggen.

Op Productie kan men alleen inloggen met behulp van eHerkenning. Op niet productie-omgevingen is het eHerkenning of username/password; eHerkenning is voor ontwikkeling niet noodzakelijk.

3.1.2 Gebruikte componenten

De BZV-website is geschreven met een aantal componenten:

- NuGet (licentie-vrij)
- EPPlus (licentie-vrij; is overheidsinstelling)
- Connectis eHerkenning SDK voor eHerkenning (licentie-vrij)
- DevExpress (ASP .Net licentie benodigd), voor weergave componenten
- Limilabs (ontwikkelaarslicentie benodigd) voor het versturen van emails
- .NET Smtip

Er wordt voor de database ontsluiting gebruik gemaakt van Entity Framework 6 (deze versie krijgt geen updates meer).

Voor de schermelementen wordt er gebruik gemaakt van DevExpress versie 22; dit betreft hier vooral de lijstweergave en invoervelden.

Voor de website wordt gebruik gemaakt van pre-compilatie zodat build-time validatie uitgevoerd wordt en de views gecached kunnen worden voor een betere performance.

3.1.3 Indeling oplossing (.sln)

Er zijn 4 globale functionele onderdelen te onderscheiden:

- Openbare gedeelte (zonder authenticatie), met hierin ook een proef-rekenmodule
- Besloten gedeelte (met authenticatie)
 - o Adviseur/veehouder
 - o Omgeving gemeente/gemandateerde
 - o Omgeving functioneel beheerder.

De website heeft voor de beheer-module een aparte area. De andere pagina's zijn alleen direct onder de applicatie geplaatst.

De oplossing heeft de volgende projecten:

Project	Doel
BZV.Core.Common	Attributen, fout-afhandeling, standaard zaken.
BZV.Core.Controls	Standaard inrichting, gebruikte componenten, html-helpers.
BZV.Core.Data	Entiteiten en context EF6 (database first).
BZV.Core.Data.Consts	Constanten.
BZV.Core.HtmlHelpers	Html helpers.
BZV.Core.Jobs	Taken.
BZV.Core.Models	Modellen.
BZV.Core.Navigation	Navigatie helpers / menu-aansturing.
BZV.Core.Security	Beveiliging van website / email links.
BZV.Database.Development	Database project.
BZV.Reporting	PDF Veehouder Rapporten.
BZV.Website	De website.
BZV.Website.Tests	Een klein aantal automatische tests.
BZV.WebsiteHerkenning	De website voor de eHerkenning.

De oplossing is hiermee tamelijk eenvoudig ingericht.

4 Taken

Er is maar 1 taak en die voert het versturen van emails uit die in de queue staan. Deze taak is nog nooit gebruikt, maar wordt wel onderhouden.

5 Website eHerkenning

5.1 Doel

Het doel van deze website is beheer gebruik, om meta-data te verkrijgen zonder de website te vervangen indien certificaten vervangen moeten worden. In hoofdstuk 12 wordt dit verder uitgewerkt.

5.2 Gebruikte componenten

De eHerkenning-tool-website is geschreven met een aantal componenten, namelijk:

- NuGet (licentie vrij)
- Connectis eHerkenning SDK voor eHerkenning (licentie vrij).

6 WEBSITE BZV

6.1 Gebruikers

De BZV Website kent verschillende gebruikersrollen:

Rollen	Toelichting
Publiek	Kan iedereen zijn. Geen account vereist. Kan alle gepubliceerde BZV-scenario's ("Goedgekeurd-Actief") doorzoeken en de eindscore van de BZV van een bedrijf inzien.
Veehouder	Veehouder kan een BZV-scenario's aanmaken waaruit een BZV score berekend wordt. Deze kan de veehouder ook indienen. Gebruikersaccount is vereist. Deze personen staan in de tabel gebruikers en relaties
Adviseur	Door veehouder gemachtigde adviseur. De adviseur kan bij dezelfde scenario's als de veehouder en kan ook BZV-scenario's aanmaken en indienen namens de veehouder. Gebruikersaccount is vereist. Deze personen staan in de tabel Organisaties.
Gemeente	Controleert en beoordeelt BZV-scenario's, keurt ze goed of af. Bij de rol gemeente zijn er twee soorten gebruikers. - Gebruikers die geautoriseerd zijn voor één gemeente. In het systeem gekoppeld aan één gemeente. Over het algemeen is dit een medewerker van de gemeente gekoppeld aan de eigen gemeente. - Gebruikers die geautoriseerd zijn voor meerdere gemeentes. In het systeem gekoppeld aan meerdere gemeentes. (zie F.O.) Over het algemeen is dit een medewerker van de Omgevingsdienst of een samenwerkingsverband. Gebruikersaccount is vereist. Deze personen staan in de tabel gebruikers
Beheerder	De beheerder heeft specifieke rechten om administratieve taken op de webapplicatie https://bzv.brabant.nl uit te voeren. De beheerder kan elk bedrijf met bijbehorende scenario's inzien en aanpassen, maar kan ook zaken achter de schermen aanpassen zoals: <u>Gebruikers toevoegen en koppelen aan bedrijven of verwijderen;</u> <u>Nieuwe versie BZV aanmaken;</u> <u>Vragen bij de maatlatten toevoegen, aanpassen of verwijderen;</u> <u>Certificaten toevoegen (al dan niet voor bepaalde diercategorieën of op stal- of bedrijfsniveau) of verwijderen.</u> <u>Certificaten koppelen.</u> <u>Monitoringsgroepen aanmaken.</u> <u>Look en feel aanpassen, inclusief panelen.</u> Gebruikersaccount is vereist. Deze personen staan in de tabel gebruikers
Provincie Noord-Brabant medewerkers	Wordt niet gebruikt

Alle gebruikers hebben 1 rol, er is geen combinatie mogelijk. Alle nieuwe gebruikers worden opgeslagen in een tabel 'Aanmeldingen'. Een aanmelding vindt automatisch plaats zodra er een eHerkenningverzoek binnenkomt van een niet bestaande gebruiker. Een aanmelding heeft een status; deze zijn aanwezig in de tabel AanmeldingStatus.

Een aanmelding wordt automatisch gekoppeld mbv de KvK op de tabellen Organisatie, Samenwerkingsverband en gemeente. De rol wordt daarmee ook automatisch bepaald (indien mogelijk en nodig). De rol veehouder wordt dan toegekend.

Zodra een aanmelding is goedgekeurd wordt de gebruiker aangemaakt in de tabel gebruikers. Wanneer een gebruiker ingelogd is en een scenario selecteert wordt dit geadministreerd in de tabel GebruikerHeeftScenario.

Een relatie is een veehouderbedrijf (ook locatie genoemd). Deze wordt door het BZV-Team beheerd. Een relatie kan ook 1 of meer KvK nummers hebben. Deze worden daarom in een aparte tabel RelatiesKvK opgeslagen.

Elke inlogpoging van een gebruiker wordt opgeslagen in een log (ActivityLog); hierin staan ook andere log-gegevens.

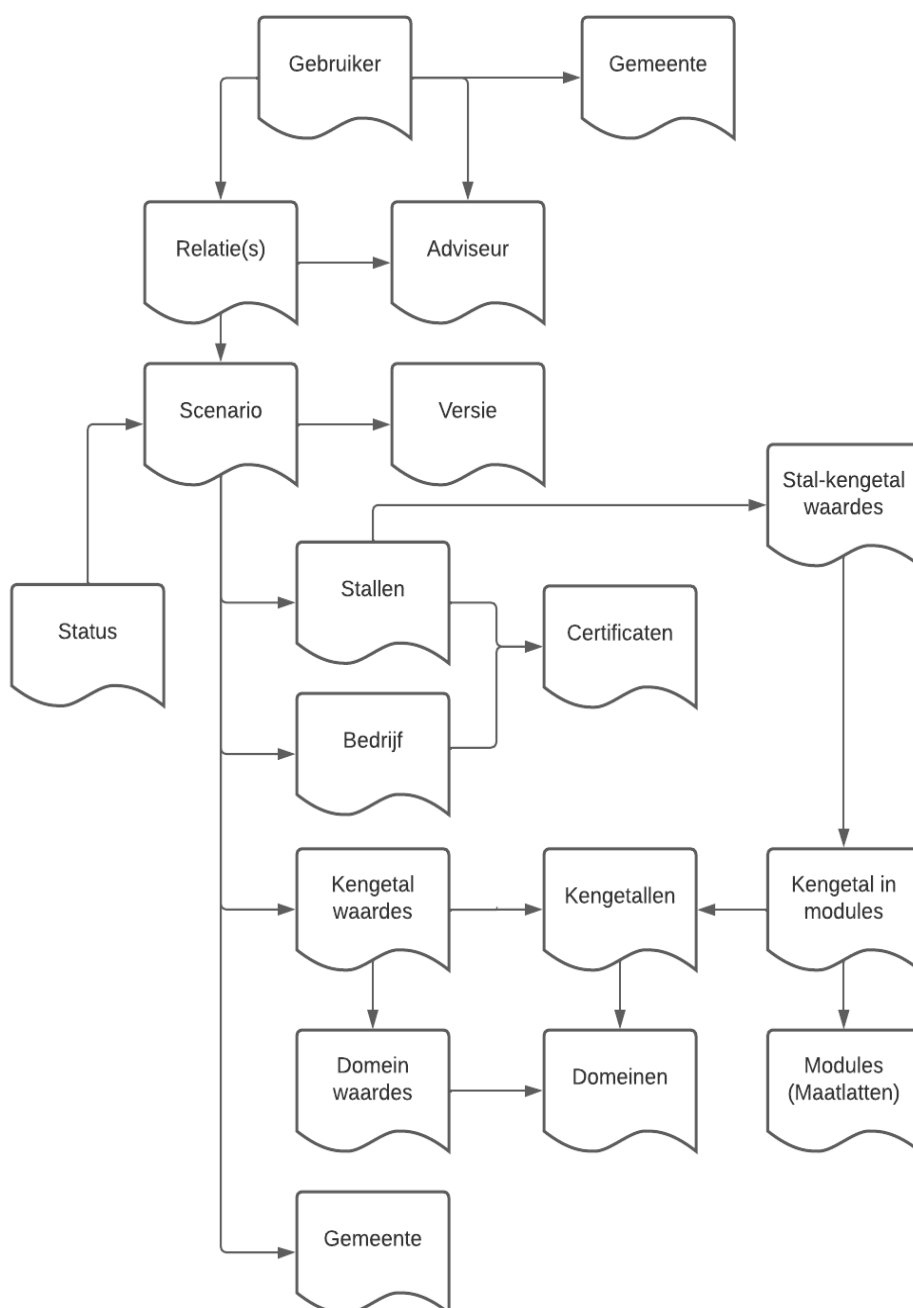
De volgende tabellen zijn in gebruik:

- Aanmeldingen
- AanmeldingStatus
- ActivityLog
- Gebruikers
- GebruikerHeeftScenario
- Relaties
- RelatiesKvK
- Gemeente
- Samenwerkingsverbanden
- Organisaties

6.2 Scenario's

De website draait vooral om scenario's. Een scenario is kortweg situatie-invoer van een veehouder (eventueel ondersteund door een adviseur) met hierin vragen en antwoorden. Er zijn verschillende soorten vragen en deze zijn gegroepeerd. Deze groepering heet een maatlat. De maatlatten zijn opgeslagen in de tabel Modules

Vereenvoudigd datamodel over scenario's



Er zijn technisch geen verschillende soorten scenario's. Door een speciale gebruiker en relatie zijn er proefberekeningen(proefscenario's) of gedeelde scenario's mogelijk. De relatie met code 9999ZZ99 is hiervoor aangemaakt. In de code wordt deze relatie uitgesloten van beheermogelijkheden en van scenario-selectie/weergave.

6.3 Modules/maatlatten

Er zijn verschillende invoer-modules, oftewel maatlatten. Onder BZV zijn de volgende maatlatten geconfigureerd:

TOP_BZV	Top-module Invoer BZV
IN_BZV_BAS	Basisgegevens
IN_BZV_GZH	Gezondheid
IN_BZV_FIJ	Fijnstof
IN_BZV_VBG	Verbinding
IN_BIODIV	Biodiversiteit
IN_BZV_BIO	Biodiversiteit
IN_BZV_MKP	Mineralenkringloop
IN_BZV_AMM	Ammoniak
IN_BZV_GCT	Geurimpact
IN_BZV_GEU	Geuremissie
IN_BZV_CTF	Certificaten
BEDRIJF	Bedrijf
IN_BZV_STA	Stalgegevens
IN_BZV_INN	Innovatie
BZV_NG_BEDRIJF	Gezondheid bedrijfsniveau
BZV_NG_DSOORT	Gezondheid diersoortniveau
BZV_NG_STAL	Gezondheid stalniveau
BZV_BIO_TOT	BZV Biodiversiteit totaal
BZV_VMOMG_TOT	BZV Verbinding totaal
BZV_CRT_STAL	BZV Certificaten stalniveau
BZV_RESULTAAT	Bevat parameters voor het berekenen van het resultaat
BZV_CRT_RESULTAAT	BZV Certificaten resultaat
BZV_CRT_BEDRIJF	Certificaten bedrijfsniveau
BZV_CRT_DSOORT	Certificaten diersoortniveau
BZV_RAP_BASGEG	BZV Rapportage basisgegevens
BZV_RAP_ADV	BZV rapportage basisgegevens adviseur

Binnen een module wordt via de tabel kengetallen_in_module aangegeven welke kengetallen hierbinnen vallen. De kengetallen zijn vooral bedoeld voor vragen of totalen. Certificaten zijn een uitzondering. Deze worden niet via kengetallen aangestuurd, maar via speciale certificaat-tabellen. De uitslagen van certificaten, worden wel in kengetallen opgeslagen en zijn dan ook te vinden in een module (bijvoorbeeld BZV_CRT_BEDRIJF).

6.4 Kengetallen

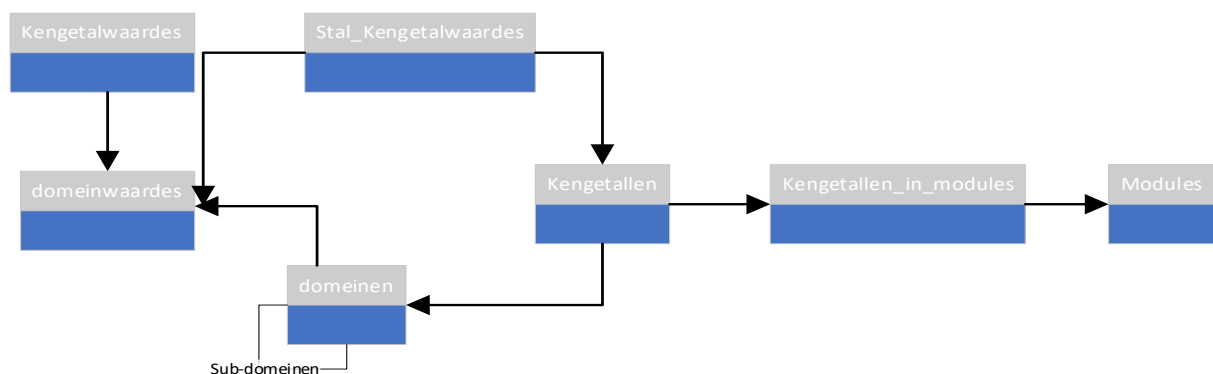
Er zijn veel verschillende kengetallen, ze kunnen in 2 groepen ingedeeld worden, namelijk vragen en uitslagen.

Een vraag is bijvoorbeeld “hoeveel huizen staan op uw weiland?”. Hierop kunnen verschillende antwoorden gegeven worden. Welke antwoorden dat zijn wordt bepaald door het gekoppelde domein.

De keuze die een gebruiker maakt op het antwoord wordt opgeslagen in kengetalwaardes (gekoppeld aan scenario) of in stal_kengetalwaardes (gekoppeld aan stal en scenario).

Het antwoord van een kengetal wordt opgeslagen in het veld Domeinwaardeld, DecimalValue, TextValue of DateValue. Een combinatie van de twee (de punten uit de domein waarde in DecimalValue en de verwijzing ook naar DomeinWaardeld)

Kengetalwaardes zijn gekoppeld aan het kengetal en aan de domeinwaarde-tabel. Via het veld waarde in kengetalwaardes (een unieke code per domeincode) is domeinwaardes(kolom waarde) gekoppeld. Het waarde veld staat op de nominatie om in nieuwere versies te verdwijnen.



6.5 Domeinen

Domeinen kunnen veelal beschouwd worden als de antwoordmogelijkheden op vragen.

Een domein bevat weinig eigenschappen, namelijk:

1. Een domeincode
2. Een vervolg domein-code
3. Een omschrijving
4. Een type

De domeincode is uniek. Het domein vervolg bevat veelal verkeerde gegevens. De referentie integriteit is niet afgedwongen. Dit zal in een volgende versies niet langer meer het geval zijn.

De omschrijving wordt soms gebruikt om weer te geven, meestal is dit alleen een informatie-veld.

Het type-veld kan het volgende bevatten:

- N (Numeriek)
- T (Tekst)
- A (Alfa-numeriek, korte tekst)
- D (Datum)
- B (Boolean)

Een domein heeft verschillende antwoord mogelijkheden. Deze staan in domeinwaardes. Domeinwaardes zijn per versie instelbaar.

Domein code	
Vervolg domein	
Filtercode	Een filter mogelijkheid
Volgorde	Volgorde
Omschrijving	Antwoord / Omschrijving
Punten	(was extra_kenmerk1)
SectorId	Sector Id voor dier-sectoren
Extra_kenmerk2	
Extra_kenmerk3	
Versie	

Een vervolg domein is voor punten bepaling. Stel je hebt een vraag (Domein) met 2 antwoorden (ja/nee), maar per sector kan je andere punten geven. Het is dan zo opgezet dat Ja niet herhaald wordt, maar dat ja voor de sectoren in een ander domein met sectorId gevuld dan de punten bevat.

7 PARAMETERS

Voor de rekenmodule zijn er bepaalde instellingen die per versie kunnen verschillen. Daarom is er een parameter tabel waarin de verschillende parameters benoemd zijn en een parameterwaarde tabel met hierin de waarde per versie. Vanaf versie 4.5 zijn dit alleen numerieke waarden, en daarom wordt dit als enige ondersteund.

8 NAVIGATIE

De navigatie door het systeem en wat weer te geven wordt bepaald door de menu-item-tabel, de sidepanelpanel, de legenda tabel, de menu-item koppel tabel naar side-panels en legenda's.

De beheerschermen zijn niet opgenomen in het menu-item en ondersteunen ook geen legenda of side-panel. Via de Css instellingen is deze ook extra breed zodat er voldoende informatie op de schermen passen. Er is hierbij wel rekening gehouden met de omgeving van de beheerders van BZV die niet de grootste schermen hebben.

9 BEVEILIGING

De authenticatie op inloggen bij de applicatie is geregeld via eHerkenning; waarbij wordt vergeleken met de bijbehorende sleutels in de gebruiker-tabel. De autorisatie om wat te mogen uitvoeren is per pagina geregeld.

De scenario pagina's mogen zowel door publieke gebruikers als door ingelogde gebruikers gebruikt worden en zijn geheel gelijk, een paar onderdrukkingen daargelaten. Voor elke rol zijn er eigenstart pagina's; elke pagina heeft controle of de gebruiker ingelogd moet zijn en (optioneel) of er een scenario geselecteerd dient te zijn. Hierop wordt op elke website aanroep of api-call gecontroleerd. Er wordt hierbij wel gebruik gemaakt van basis-laag-controllers zodat deze code niet vergeten wordt.

10 REKENMODULE

De rekenmodule is behoorlijk complex en daarom worden in dit hoofdstuk alleen de hoofdlijnen behandeld. Alle procedures, functies en tabellen zijn inzichtelijk via SQL Management studio, maar ook via het project BZV.Database.development waarop alle meta-data (structuren, tabellen, functies, view, etc) de gehele ontwikkelomgeving is opgenomen.

Elke module/maatlat heeft zijn eigen uitkomsten. We richten ons hier op de belangrijkste:

- Certificaten
- Gezondheid
- Verbinding

Certificaten en gezondheid kunnen verder verdeeld worden over:

- Bedrijf
- Stal (per unieke stalafkorting)
- Diersoort

De rekenmodule zit geheel in T-SQL code en start met:

```
Exec [dbo].[BZV_bereken_scenario_resultaatV2] @ScenarioID int = ScenarioID= 'Calculate', @CalculationType,  
@VergelijkingId = null
```

Deze procedure heeft als ingang het scenario. De CalculationType kan zijn CALCULATE, RETRIEVAL of CalculateNoLock.

Calculate is de standaard en zorgt ervoor dat de berekening binnen een transactie uitgevoerd wordt, opgeslagen en geretourneerd. Indien de status van het scenario niet concept en niet zandbak (proefberekening) is, dan wordt er geen berekening uitgevoerd. De optie RETRIEVAL wordt dan uitgevoerd.

Retrieval zorgt ervoor dat de berekeningsresultaten worden teruggestuurd. Er wordt dus niets berekend.

CalculateNoLock is voor test- en onderzoeksdoeleinden, er wordt gebruik gemaakt van een uncommitted transactie en dus is de juistheid niet gegarandeerd als ook andere personen binnen het systeem wijzigingen maken; het is ook niet belemmerend voor deze gebruikers.

De berekeningsroutine moet geschikt blijven voor alle BZV-versies.

De berekeningsresultaten worden in kengetalwaardes opgeslagen. Alle kengetallen voor dit doeleinde starten met RES_ naamgeving.

De berekening houdt ook rekening met eventuele correcties. Indien er configuratie is aangepast, dan worden er mogelijk ook antwoorden op vragen die eigenlijk niet gesteld hadden moeten worden verwijderd.

De berekening start verder de maatlatten berekening procedure en slaat daarna eventuele aanvullende afwijkingen/resultaten op. De maatlatten berekening is procedure **BZV_bereken_scenario_maatlatten**.

Deze functie kan aangeroepen worden met @RetrieveOnly. Indien deze 1 is, dan worden de procedures **BZV_bereken_Scenario_certificaatresultaat** en **bzv_bereken_scenario_gezondheidResultaat** niet aangeroepen en de kengetallen met de totalen worden teruggestuurd.

In het andere geval worden alle punten verzameld en in de totalen kengetallen geplaatst. Bijna alle kengetallen voor de totalen zijn eindigend met TOTAAL of TOTAAL_ORG. Totaal zijn de totalen in de kengetallen die uiteindelijk toegekend worden, zonder correcties. TOTAAL_ORG zijn de totalen die nog niet gecorrigeerd zijn (doordat bijvoorbeeld maximum overschreden is).

Bij het berekenen wordt gebruik gemaakt van de volgende twee functies:

- **BZV_scenario_kengetal_punten**
- **BZV_scenario_kengetal_puntenV2**

Beide functies bereken bijna hetzelfde, vanwege performance bestaan er echter 2. De voorkeursmethode is versie 2. In de functies worden de kengetallen van de modules (voorwaardelijk) opgeteld.

De 2 versies zijn vooral anders vanwege vraag 4 van de gezondheidsvragen. Deze heeft een nogal afwijkende configuratie.

11 CERTIFICATEN

Er zijn per omgeving een aantal certificaten nodig. Op de ontwikkelomgeving zijn er geen nodig.

We beschrijven hier de certificaten die verplicht zijn voor productie.

1. Web site SSL. Maximale duur 3 jaar.
 - PKI Overheidscertificaat (KPN PKIoverheid Server CA 2020).
 - Besteld de provincie Noord Brabant.
 - Server (SSL) - certificaat
2. eHerkenning SSL van de server (PKI). Maximale duur 1 jaar.
 - PKI Overheidscertificaat (KPN PKIoverheid Private services CA - G1).
 - Besteld de provincie Noord Brabant.
 - Server (Machine) - certificaat
3. eHerkenning SSL van Connectis (PKI). Maximale duur 1 jaar.
 - PKI Overheidscertificaat (QuoVadis PKIoverheid Server CA 2020).
 - Regelt de leverancier (geen kosten)
 - Client (Machine) - certificaat

Het certificaat van de eHerkenning is niet geschikt voor websites en daarom kunnen deze niet hergebruikt worden.

12 EHERKENNING

De eHerkenningsmodule is eenvoudig en is afkomstig van Connectis¹. Er is voor de code echter geen documentatie beschikbaar en de informatie op het internet van Connectis over deze code sluit niet aan bij de werking van de methoden/configuratie (bepaald per Q2 2022).

Deze module heeft een paar functies en het enige dat voor de website gebruikt wordt is inloggen. Voor niet-productie-omgevingen kan de eHerkenning uitgezet worden of dual ingezet worden; er wordt dan gebruik gemaakt van gebruiker/password mogelijkheid.

De certificaten van de website moeten onder de gebruiker van de IIS-website in de *personal store* geïnstalleerd worden met volle rechten. Tevens moeten het certificaat van de Connectis daar beschikbaar zijn.

De Connectis software werkend krijgen is vaak een ander verhaal. Omdat bij gebruik bijna nooit duidelijk is wat de veroorzaker van de fout is. Je kan hierbij denken aan:

- Firewall blokkades
- DNS
- Benodigde encryptie modules op de server. Windows Server 2019 minimaal.

¹ Tegenwoordig Signicat, maar bij de software heet dit nog steeds Connectis.

- De tijd mag niet te veel afwijken (120 seconden maximaal) van de Connectis servers en moet dus bewaakt worden met een tijddienst.

12.1 Dienstverlener inrichting

De dienstverlener van de eHerkenning is de Provincie Noord Brabant. In BZV zijn er een aantal bestanden (voor acceptatie en productie een eigen set):

1. levelOfAssurances.xml
2. services.xml
3. urn_eToegang_DV.xml
4. urn_eToegang_HM.xml
5. voor Signicat metadata.xml

Bestanden 1, 2 en 3 zijn voor de dienstverlener inrichting. In dit bestand staat aangegeven welke authenticatie mogelijkheden er zijn. In services wordt hiernaar verwezen; De tag **LevelOfAssurance** geeft aan welke authenticatie methode minimaal gebruikt moet worden.

Omdat de diensten van BZV niet de enige zijn, maar ook andere PNB sites van de dienstencatalogus gebruiken, gebruiken wij alleen dienst #4 entiteit **urn:etoegang:DV:00000003172787180000:entities:0002**. Signicat gebruikt **urn:etoegang:HM:00000003244440010000:entities:0113**.

De gegevens in bestanden 1 en 2 wijzigen eigenlijk nooit. In het derde bestand kan je meer aangeven:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceProvider>
  <ServiceProviderDefinition
    entityId="urn:etoegang:DV:00000003172787180000:entities:0002"
    contactEmail="Beheerder email adres"
    contactName="Beheerder naam"
    contactPhone="Beheerder telefoon"
    organizationName="Provincie Noord-Brabant"
    organizationDisplayName="Provincie Noord-Brabant"
    organizationUrl="www.brabant.nl"
    assertionConsumerServiceUrl="https://bzv.brabant.nl/eherkenning/acs"
    singleLogoutServiceUrl="https://bzv.brabant.nl/eherkenning/slo"
    signingKeyName="3E118DA6E926BA9D8A3963E53DD852740ED663A2"
    encryptionKeyName="3E118DA6E926BA9D8A3963E53DD852740ED663A2"
    notBeforeGracePeriodInSeconds="120"
    polymorphicKeyEndpointUrl="https://eh01.connectis.nl/broker/bsnk"
    polymorphicKeyLocation="/configuration/Productie/keys/"
    sslKeyName="3E118DA6E926BA9D8A3963E53DD852740ED663A2"
    artifactResolutionServiceUrl="https://bzv.brabant.nl/eherkenning/acsart">
  </ServiceProviderDefinition>
  <Bindings>
    <SupportedBindings>
      <Binding>urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST</Binding>
      <Binding>urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect</Binding>
      <Binding>urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact</Binding>
    </SupportedBindings>
    <PreferredBinding>urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Artifact</PreferredBinding>
  </Bindings>
  <ArtifactResolutionServiceIndex>1</ArtifactResolutionServiceIndex>
  <DefaultServiceIndex>4</DefaultServiceIndex>
</ServiceProvider>
```

De organisatie naam kan niet zomaar aangepast worden. De velden met 3E118DA6E926BA9D8A3963E53DD852740ED663A2 moeten allen gelijk zijn.

Let op: Het is mogelijk dat Signicat medewerkers dit tegenspreken, maar uit ervaring blijkt dat het noodzakelijk is de velden gelijk te houden!

Deze gegevens kunnen met de meta-data aanlevering bij een nieuw eHerkenningcertificaat op de webserver aangeleverd worden.

12.2 Nieuwe Signicat certificaten

Elk jaar worden er nieuwe certificaten door Signicat aangeleverd. Deze moeten exportable worden geïmporteerd in de user- en computer store van de gebruiker van de website.

Zorg ervoor dat de rechten van de eHerkenning SSL certificaat toegekend aan de gebruiker van de website (application pool)

Met de eHerkenningswebsite kan men de configuratie aanpassen.

In BZV zijn er een aantal bestanden (voor acceptatie en productie een eigen set):

1. levelOfAsurances.xml
2. services.xml
3. urn_eToegang_DV.xml
4. urn_eToegang_HM.xml
5. voor Signicat metadata.xml

Bij een nieuw certificaat (soms op verzoek van Signicat) moet de nieuwe meta-data van handelsmakelaar Signicat worden gedownload. Deze moet geplaatst worden over bestand 4 (urn_eToegang_HM.xml). Voor pre-productie (acceptatie) is deze te downloaden op:

<https://eh.pre.signicat.nl/broker/sp/eh/1.13/metadata>

voor productie is deze te downloaden op:

<https://eh.signicat.nl/broker/sp/eh/1.13/metadata>

Als het goed is, is het plaatsen genoeg om de werking te behouden. Indien de beveiliging is aangepast en andere encryptie cyphers worden gebruikt, moeten deze ondersteund worden op de server. Indien de cyphers niet ondersteuning worden komt hiervan geen foutmelding. Het bereiken van de Signicat server wordt afgewezen en daar moet je het mee doen. Neem na problemen met het nieuwe certificaat contact op met Signicat. Zij hebben meet-instrumenten of nieuwere versies van de Signicat software.

12.3 Nieuw eHerkenningcertificaat WebServer

Het SSL PKI Certificaat van de eHerkenning moeten jaarlijks vervangen worden. Importeer het nieuwe certificaat exportable in de user- en computer store van de gebruiker van de website en de eHerkenningswebsite.

Zorg ervoor dat de rechten van de eHerkenning SSL certificaat toegekend aan de gebruiker van de website (application pool)

Let op! De website en de eHerkenning mogen formeel niet hetzelfde certificaat zijn volgens Signicat; maar zij spreken elkaar daarin heel erg tegen. Werkend met 2 certificaten is niet gelukt met de software van Connectis.

Na het plaatsen van het nieuwe certificaat, moet er nieuwe meta-data naar Signicat verstuurd worden. Deze kan men maken met de eHerkenningswebsite. Het beste kan de eHerkenningswebsite binnen de BZV-applicatie draaien en gestart/gestopt worden tijdens het verkrijgen van deze gegevens.

Start deze website en download de meta-data en plaats deze over de configuratie bestanden #5.

1. levelOfAsurances.xml
2. services.xml
3. urn_eToegang_DV.xml
4. urn_eToegang_HM.xml
5. voor Signicat metadata.xml

Dit bestand moet vervolgens aangeleverd worden aan Signicat. Hierbij hoort formeel ook de dienstencatalogus. Dit verzorgt SLTN niet. BZV deelt namelijk de eHerkenning met andere diensten van de provincie Noord-Brabant.

Stuur daarom een email naar Signicat met de volgende strekking:

Beste,

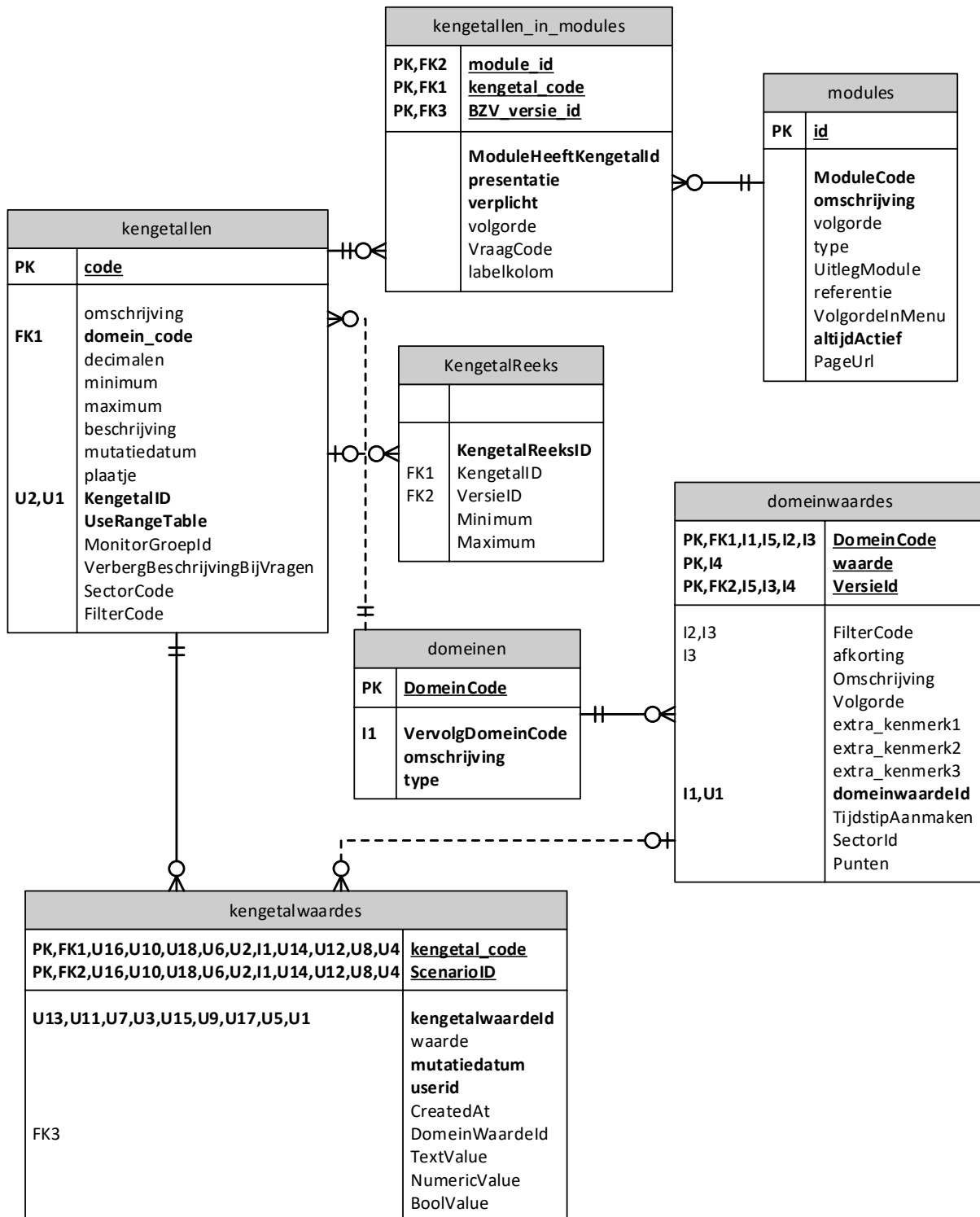
Vanwege een nieuw certificaat op onze server wil ik hierbij de nieuwe meta-data aanleveren voor onze pre-productie omgeving van BZV. Het certificaat met thumbprint
6177b9581809bbe6eee9961d14427317c5d2f3f9
word aangepast naar
8672cdef272b2b67169e145efcc6489e880dc370

Ik heb geen dienstencatalogus aangeleverd, omdat verschillende afdelingen gebruik van de diensten. Gezien de dienst alleen wijzigt voor het genoemde vingerafdruk, is dat mogelijk ook niet nodig en kunt u deze doorvoeren?

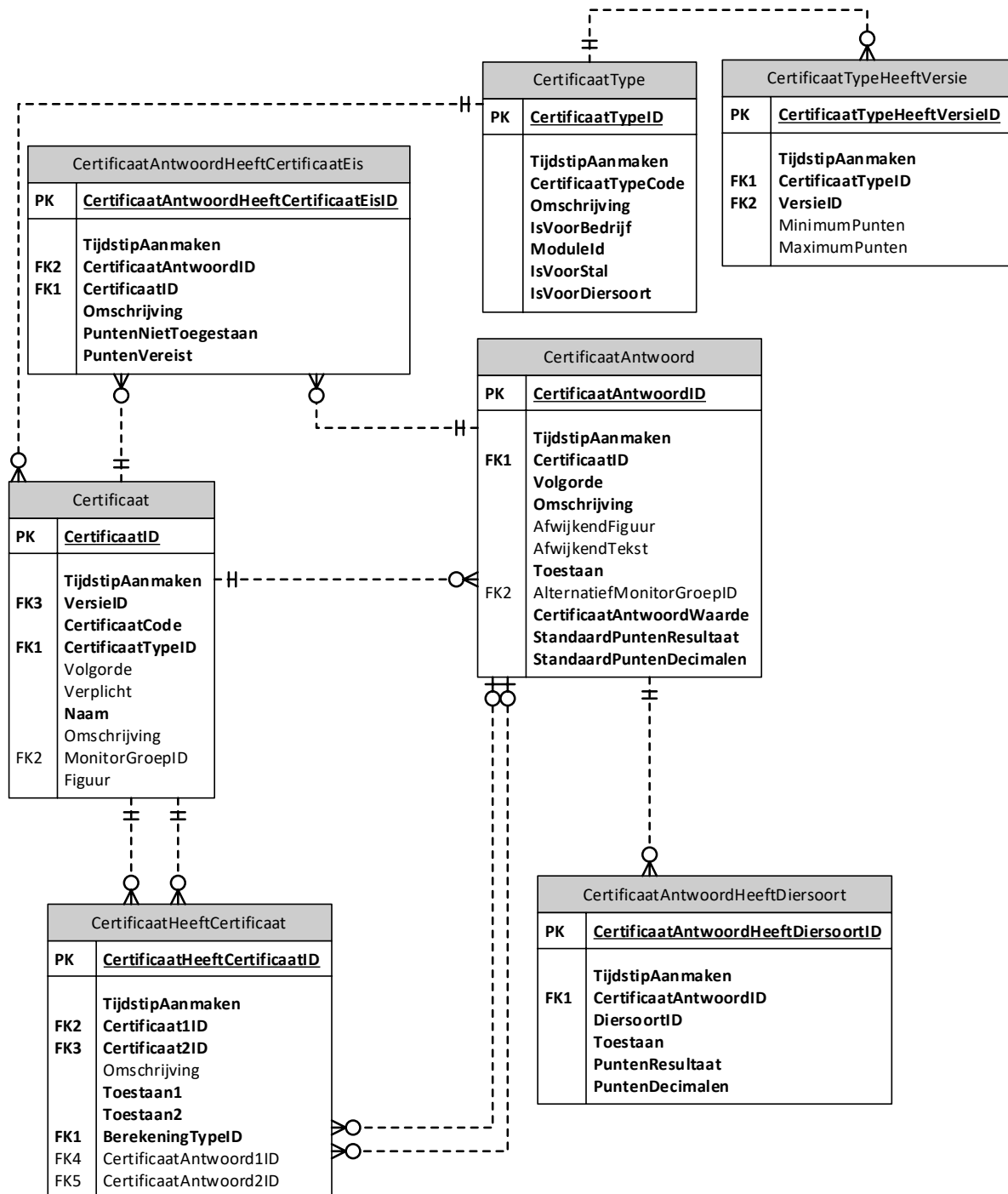
Kan deze nieuwe meta data verwerkt worden op dinsdagochtend om 09:00?

13 DATABASE ENTITEITEN MODEL

13.1 Kengetallen, modules en domeinen

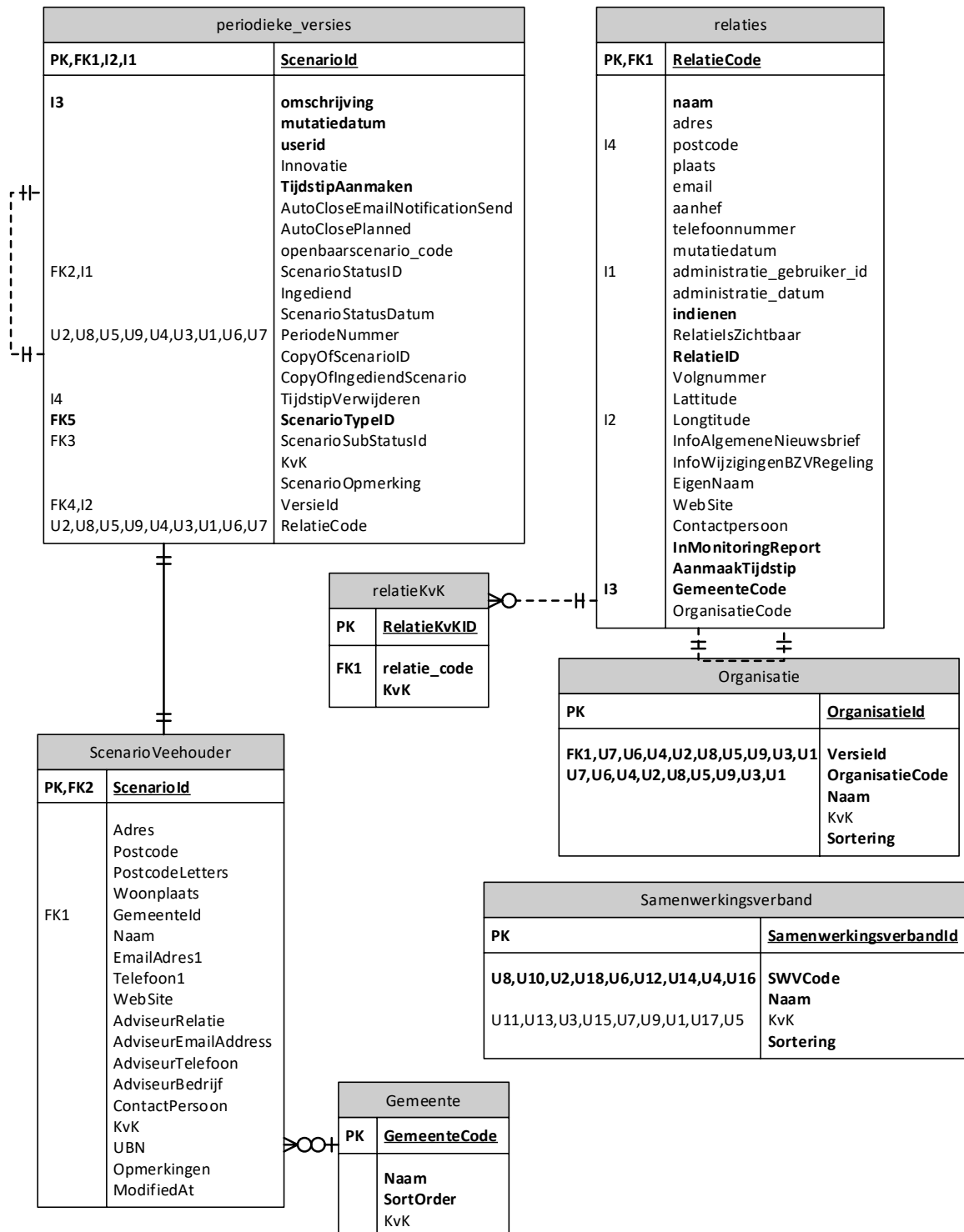


13.2 Certificaatinrichting



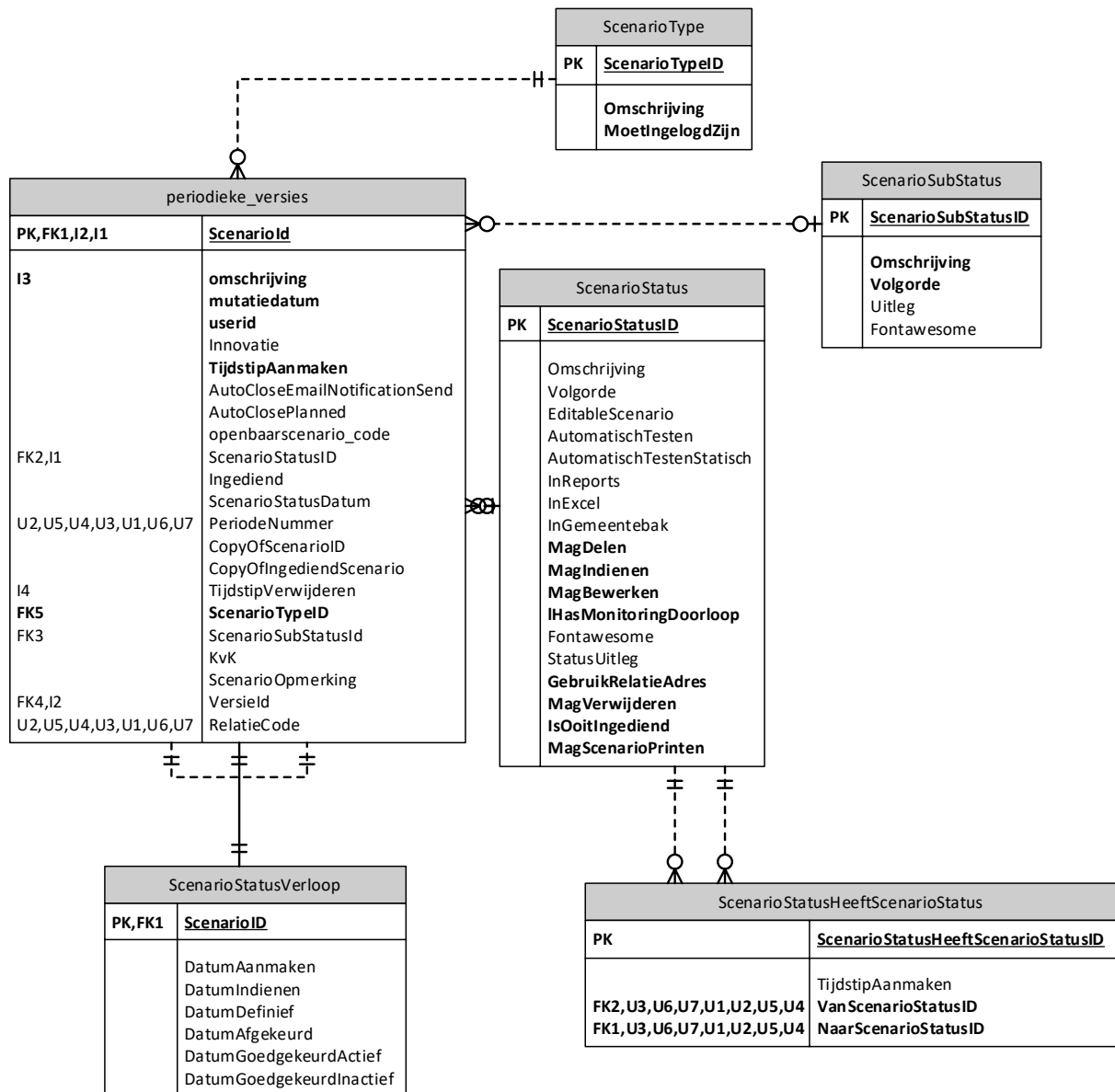
13.3 Scenario inrichting

In de basis is een scenario opgeslagen in de tabel `periodieke_versies`. Er is ook een view `Scenario` die redelijk overeenkomt met `periodieke_versies` gecombineerd met een aantal andere gegevens voor het dagelijkse gebruik. De naam `periodieke_versies` komt voor uit de oorsprong van de applicatie.



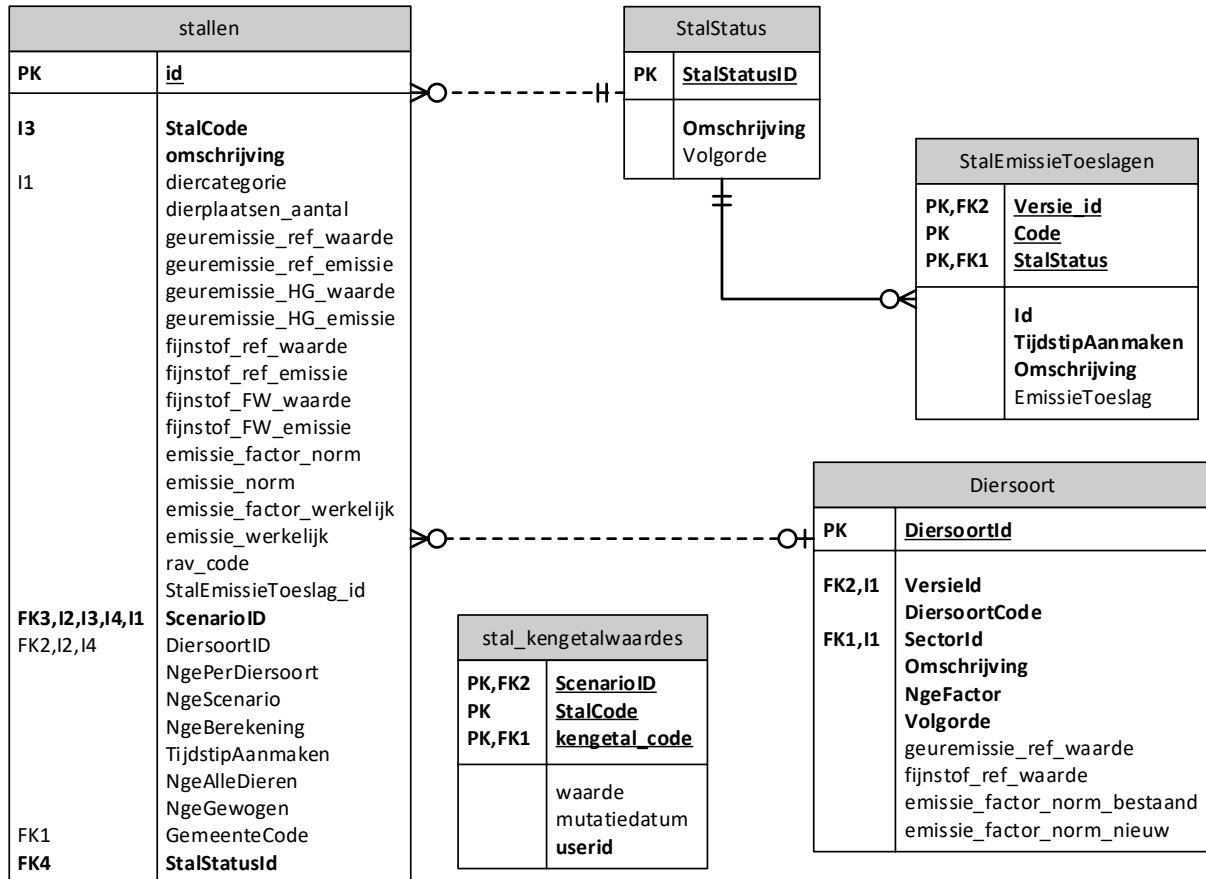
In dit overzicht ontbreken nog een aantal sleutels. Deze volgen in het eerste kwartaal van 2023 zodra deze aan het model zijn toegevoegd.

13.3.1 Scenario status / fiatterings status



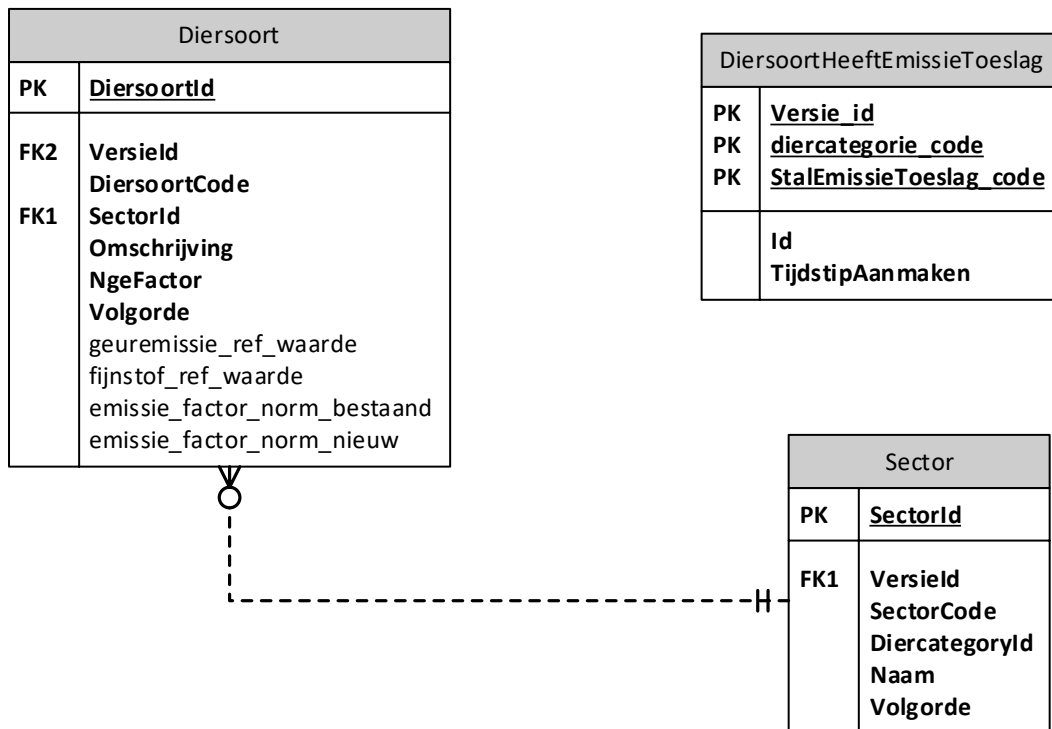
13.3.2 Scenario Stallen

De stallen zijn gekoppeld via een scenario -referentie in de stallen tabel aan periodieke versies. De stal heeft kengetalwaarden, stalemissie toeslagen en een status.



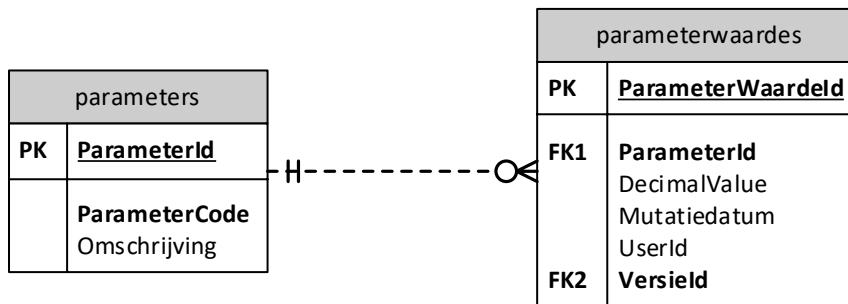
Een stal heeft een stalcode. Deze hoeft niet uniek te zijn per scenario. Een fysieke stal kan namelijk kippen en geiten bevatten. Deze hebben dan dezelfde stalcode. De stal_kengetalwaarden waarin de resultaten van vragen worden opgeslagen zijn dan ook niet verbonden aan één stalrecord, maar potentieel aan meer dan 1. Dit is ook de reden dat hier geen unieke sleutel tussen zit. Er is ook geen koppeltabel voor.

13.4 Diersoorten



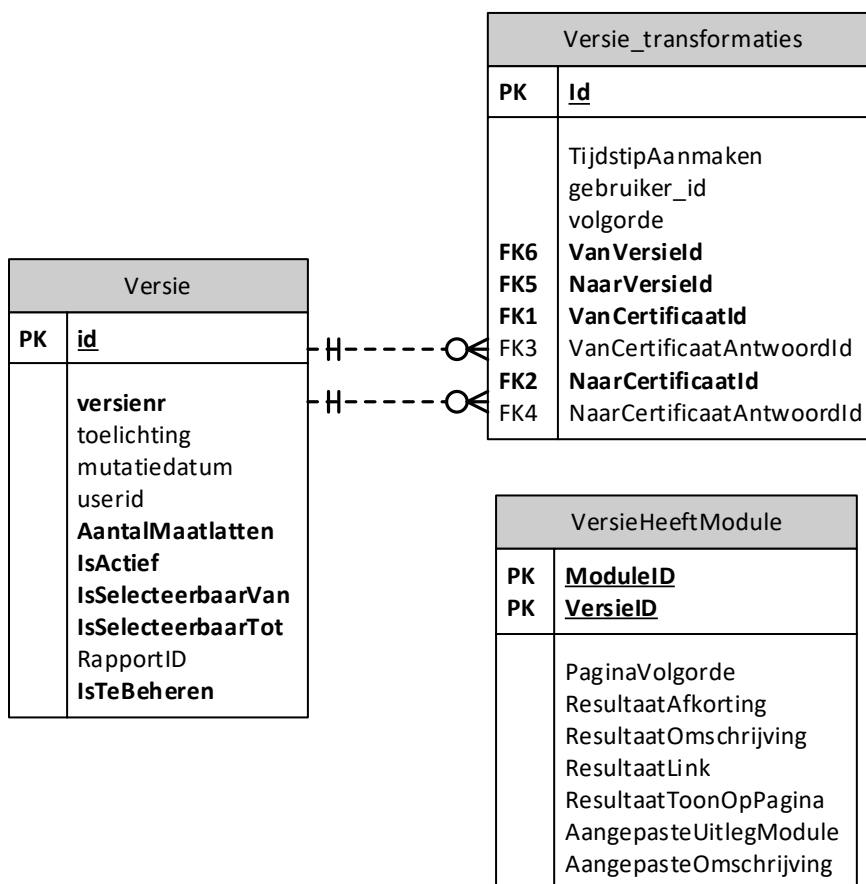
In dit overzicht ontbreken nog een aantal sleutels. Deze volgen in het eerste kwartaal van 2023 zodra deze aan het model zijn toegevoegd. Tevens is de diercategory nog bestaand. Deze zal ook verdwijnen.

13.5 Configuratie maatlatten (parameters)

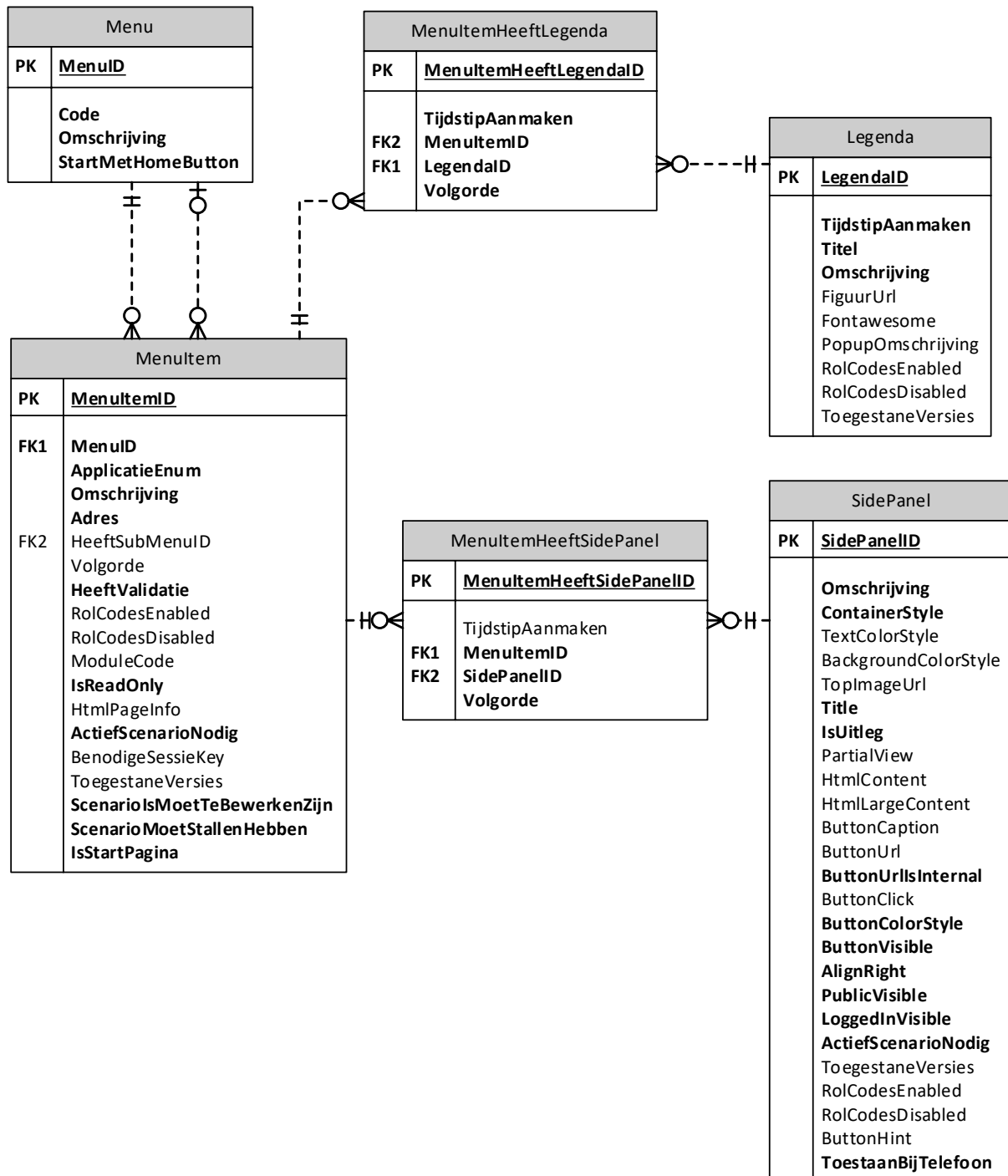


13.6 Versies

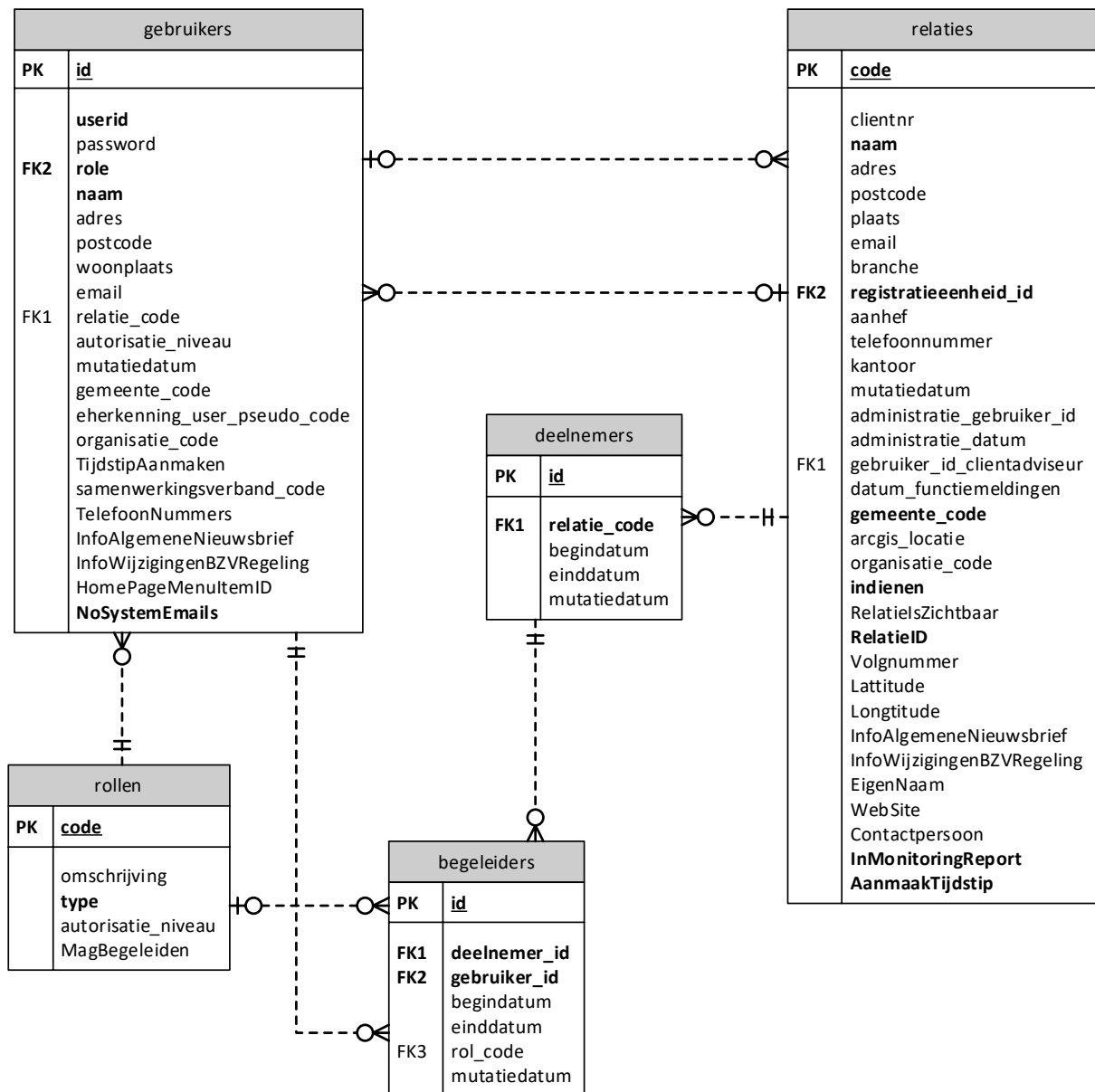
Omtrent de versies hangt heel veel samen. De samenhang weergeven in een overzicht heeft weinig meerwaarde.



13.7 Menu, legenda en sidepanels



13.8 Gebruikers



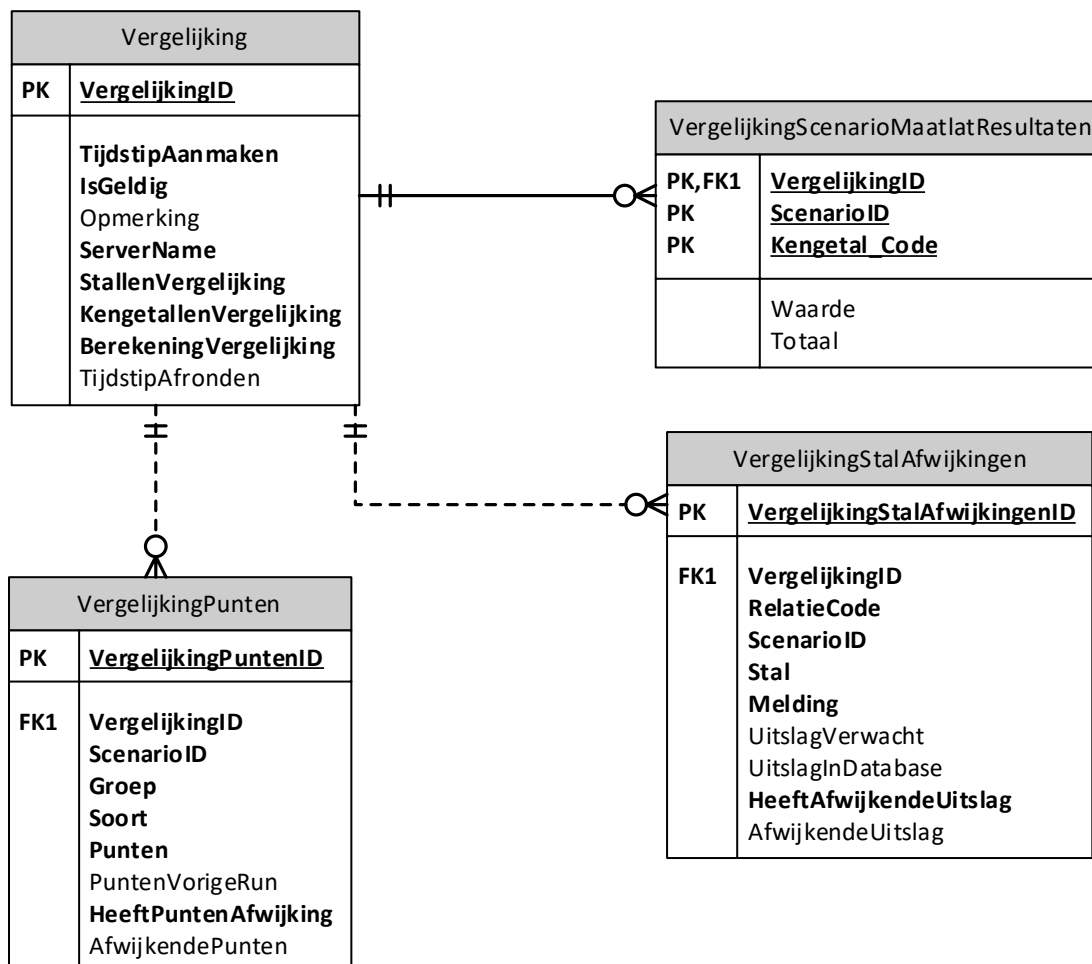
13.9 Aanmeldingen

Aanmeldingen	
PK	<u>AanmeldingId</u>
	Rolcode Naam Adres Postcode Woonplaats Telefoonnummer Emailadres Pseudoniem Kvnummer KvnummerIntern Opmerking DatumGoedkeuring Bedrijfsnaam InfoAlgemeneNieuwsbrief InfoWijzigingenBZVRegeling BevestigingsCode AanmeldingStatusId EmailText

AanmeldingStatus	
PK	<u>AanmeldingStatusId</u>
	TijdstipAan maken AanmeldingStatusCode Omschrijving IsVisible SortOrder

13.10 Vergelijkingsrapportage

Dit zijn de tabellen voor de vergelijkingsrapportage waarmee dagelijks alle scenario's worden berekend, zodat afwijkingen gedetecteerd kunnen worden (door zowel modelconfiguratie als door aanpassingen in de code, als door gebruikers).



13.11 Rapportage tabellen

MonitorGroep	
PK	<u>MonitorGroepId</u>
	TijdstipAanmaken Volgorde Omschrijving OpnemenInExcel ExcelVeldnaam StalCertificaat ExcelPositie