DDAS API Koppelvlakspecificatie

Koppelvlakspecificatie voor het beschikbaarstellen van DDAS-gegevens aan het CBS

VNG Realisatie

VNG Realisatie Standaard
In Ontwikkeling versie 11 februari 2025

Deze versie:
https://vng-realisatie.github.io/publicatie/hl/respec-template/0.21

Laatst gepubliceerde versie:
https://vng-realisatie.github.io/publicatie/hl/respec-template

Laatste werkversie:
https://govert-claus.github.io/DDAS-API/

Redacteur:
Govert Claus (Programma DDAS)

Doe mee:
GitHub Govert-Claus/DDAS-API
Dien een melding in
Revisiehistorie
Pull requests

Dit document is ook beschikbaar in dit niet-normatieve formaat: pdf

---

Samenvatting

Dit is de koppelvlakspecificatie voor de API waarmee schuldhulporganisaties gegevens beschikbaarstellen aan het CBS. Dit is een product van het programma DDAS. De API is gebaseerd op het informatie- en uitwisselmodel.

Naast de uitgangspunten en de technische specificatie bevat dit document een beschrijving van de niet-functionele eisen (beschikbaarheid, performance). Ook worden het aanleverprotocol (welke stappen worden doorlopen als gegevens opgehaald worden) en het aansluitprotocol (hoe kan een organisatie deelnemer worden) beschreven. Ten slotte wordt het beheer van de specificatie zelf beschreven.

In de huidige versie staan nog diverse vraagstukken en de keuzes die gemaakt worden, moeten nog worden bevestigd. Het document dient daarom vooral als basis voor de discussie om tot een definitieve specificatie te komen, en er kunnen geen rechten aan dit document ontleend worden.

Status van dit document

Dit document is nog 'In Ontwikkeling'.

Inhoudsopgave

1. Uitgangpunten

1.1 Kaders

Het koppelvlak moet voldoen aan de volgende wetten, afspraken en standaarden:

- NORA
- BIO
- Digikoppeling – REST-API profiel
- Nederlandse API strategie
- NL Gov REST-API Design Rules
- Algemene verordening gegevensbescherming
- Wet op het Centraal Bureau voor de Statistiek

1.2 Keuzes

De volgende keuzes zijn gemaakt:

Gegevensleveranciers bieden een API aan die rechtstreeks door CBS wordt bevraagd

Rationale

- Dit uitwisselpatroon past het best bij het Federatief Datastelsel.
- Gegevens blijven in de bron en worden bevraagd als ze nodig.
- De API waarmee gegevens beschikbaar gesteld worden, kan hergebruikt worden voor andere toepassingen.
- Dit patroon is besproken in de stuurgroep van 16 december 2024 en als voorkeurspatroon geaccepteerd (rekening houdend met de kanttekeningen die in de besproken beslisnotitie zijn meegegeven).

Implicaties

- Alle gegevensleveranciers moeten een API beschikbaar stellen waar de DDAS-gegevens opgevraagd kunnen worden.
- De API moet voldoende beschikbaar zijn om CBS op de gewenste momenten te faciliteren.

Gebruik Digikoppeling REST profiel

Rationale

- Dit profiel is het minst complexe profiel voor API's en past het beste bij een stelsel waar veel partijen aan deelnemen en in eigen tempo kunnen aansluiten.

Implicaties

- Alle leverende deelnemers dienen een API conform het REST profiel beschikbaar te stellen.
- Omdat het Digikoppeling REST profiel nog geen keuze heeft gemaakt voor signing en encryptie, moet hier expliciet een keuze in gemaakt worden.

Gebruik JAdES voor signen

Rationale

- Omdat het REST profiel van Digikopeling (nog) geen standaard voor signen heeft vastgesteld, moet er een gekozen worden.
- JAdES is als standaard voorgesteld door het Kennisplatform API's.
- JAdES is gebaseerd op JWS, de standaard voor signing van REST/JSON berichten die wereldwijd breed toegepast wordt.
- JAdES plaatst het signen "naast" het bericht, zodat het bericht zelf niet beïnvloed wordt en ook zonder de signing gebruikt kan worden.

Implicaties

- Alle berichten krijgen een ondertekening door de partij die het bericht verstuurd.
- Voor ondertekenen is een certificaat nodig; alle deelnemers moeten een certificaat hebben dat vertrouwd wordt. NB: dit moet een ander certificaat zijn dan diegene die nodig is voor dubbelzijdig versleuteld transport (TLS).

Gebruik ADR-HTTP Payload encryption voor encryptie *(NB: als encryptie vereist is - de verwachting is dat dit NIET nodig is)*

Rationale

- Omdat het REST profiel van Digikopeling (nog) geen standaard voor encryptie heeft vastgesteld, moet er eentje gekozen worden.
- De "payload encryption" is als standaard voorgesteld door het Kennisplatform API's.
- De "payload encryption" standaard is gebaseerd op JWE, de internationale standaard voor encryptie die breed toegepast wordt.
- Als versleutelen nodig is, hoeven alleen de berichten waarin persoonsgegevens zitten versleuteld te worden. Dat zijn de responses van de gegevensleveranciers.

Implicaties

- Alle berichten worden versleuteld door de partij die het bericht verstuurd.
- Voor ondertekenen is een tweede certificaat nodig; dit moet een ander certificaat zijn dan het certificaat dat voor het ondertekenen gebruikt wordt. Omdat alleen de responses versleuteld worden, volstaat één extra certificaat bij CBS: het bericht wordt versleuteld met de publieke sleutel van de ontvanger (zie ook "Signing en Versleuteling").

Federatieve Services Connectiviteit voor de connectiviteit - FSC

Rationale

- Deze standaard is verplicht als het REST profiel van Digikoppeling wordt gebruikt.

- Door te kiezen voor een standaard, vereenvoudigt de complexiteit waar gemeenten met veel koppelingen mee te maken hebben.
- Er bestaat een referentie implementatie die de inrichting en het gebruik van de API sterk vereenvoudigt. Verder is er bij VNG Realisatie (waar de standaard is ontwikkeld), het Federatief Datastelsel en RINIS kennis die gebruikt kan worden.

Implicaties

- Alle deelnemers dienen de FSC componenten te installeren en in te richten. Er bestaat een algemene referentie implementatie, die waarschijnlijk zo ingezet kan worden. Als deze niet voldoet, kan overwogen worden om een specifieke referentie implementatie voor DDAS beschikbaar te stellen.
- FSC gaat uit van dubbelzijdig versleuteld transport (TLS). Hiervoor hebben alle deelnemers van het DDAS-stelsel een certificaat nodig dat vertrouwd wordt.

Gebruik van FSC directory van RINIS

Rationale

- RINIS biedt een FSC directory aan voor alle overheidspartijen die de Digikoppeling standaard voor REST API's toepassen. Ook het DDAS stelsel mag daar gebruik van maken.
- Door gebruik te maken van de directory bij RINIS is er geen beheer nodig voor de centrale directory.
- RINIS wordt gezien als onafhankelijke partner, die door alle deelnemers vertrouwd wordt.
- Door gebruik te maken van de directory van RINIS zijn de services (in principe) makkelijk te hergebruiken voor andere diensten binnen de overheid.
- RINIS biedt de mogelijkheid om een eigen omgeving voor het DDAS stelsel te gebruiken, waar eigen voorwaarden voor deelname aan gekoppeld kunnen worden. *NB: er wordt nog overwogen of dit nodig is en meer voor- dan nadelen biedt*

Implicaties

- Het koppelvlak moet voldoen aan het REST profiel van de Digikoppeling standaard en gebruik maken van PKIo certificaten (dit is een voorwaarde om gebruik te maken van de voorziening van RINIS).
- Alle deelnemers moeten hun endpoint (laten) registreren bij RINIS. Dit gebeurt als onderdeel van het aansluitprotocol en wordt gefaciliteerd door CBS of het programma DDAS.
- Voor het ophalen van de gegevens, moet CBS de directory van RINIS bevragen om de lijst endpoints op te halen.

JSON formaat voor berichten

Rationale

- Het informatiemodel en het uitwisselmodel voor DDAS zijn in het JSON formaat ontwikkeld. Het is het eenvoudigst als de berichten dan ook in JSON formaat uitgewisseld worden.
- JSON is goed leesbaar voor mensen, maar toch voldoende klein om ook grotere berichten uit te kunnen wisselen.
- Vrijwel alle moderne informatiesystemen kunnen goed overweg met JSON berichten, wat de inrichting en het beheer vereenvoudigt.

Implicaties

- De gegevens moeten in JSON formaat uitgewisseld worden.

Gebruik "open" internet voor transport

Rationale

- Een (groot) aantal deelnemers in het DDAS-stelsel heeft geen toegang tot Diginetwerk en aansluiten via een koppelnetwerkaanbieder zal onevenredig veel inspanning, doorlooptijd en kosten met zich meebrengen.
- Er zijn geen routeervoorzieningen of andere "tussenstations" in het stelsel voorzien, waardoor "Man in the Middle" aanvallen onwaarschijnlijk zijn.
- Het transport wordt met dubbelzijdig TLS versleuteld, wat voldoende beveiliging geeft.
- Middels de directory van FSC worden alleen vertrouwde endpoints aangeroepen.

Implicaties

- Aansluiten op het stelsel vereist geen toegang tot een gesloten netwerk.
- Het transport moet met dubbelzijdig TLS beveiligd worden.
- Alleen endpoints die in de directory van FSC zijn vastgelegd, worden bevraagd.

Gebruik PKIoverheid certificaten voor authenticatie, signing en encryptie

Rationale

- Voor identicatie, authenticatie, signen en encryptie is een middel nodig dat door alle deelnemers van het stelsel vertrouwd wordt. PKIoverheid certificaten worden door de Nederlandse overheid uitgegeven, die daarmee de "Trust Anchor" voor het DDAS-stelsel wordt.
- PKIoverheid certificaten worden door Logius (namens de rijksoverheid) via Logius geautoriseerde aanbieders uitgegeven en beheerd. Er is daarom geen organisatie nodig om certificaten voor het DDAS-stelsel te beheren.

Implicaties

- Alle deelnemers moeten PKIoverheid certificaten hebben of krijgen. NB: er zijn certificaten nodig voor de transportlaag en het ondertekenen van berichten (hiervoor mag niet hetzelfde certificaat gebruikt worden). Mogelijk kunnen bestaande certificaten hergebruikt worden, maar hier moet voorzichtig mee omgegaan worden om beveiligingsniveaus gescheiden te houden. Als berichten met gevoelige gegevens ook versleuteld moeten worden, is een extra certificaat bij CBS vereist. De gegevensleveranciers gebruiken dan de publieke sleutel van dat certificaat om de berichten te versleutelen.

Beveiligingsniveau BBN2

Rationale

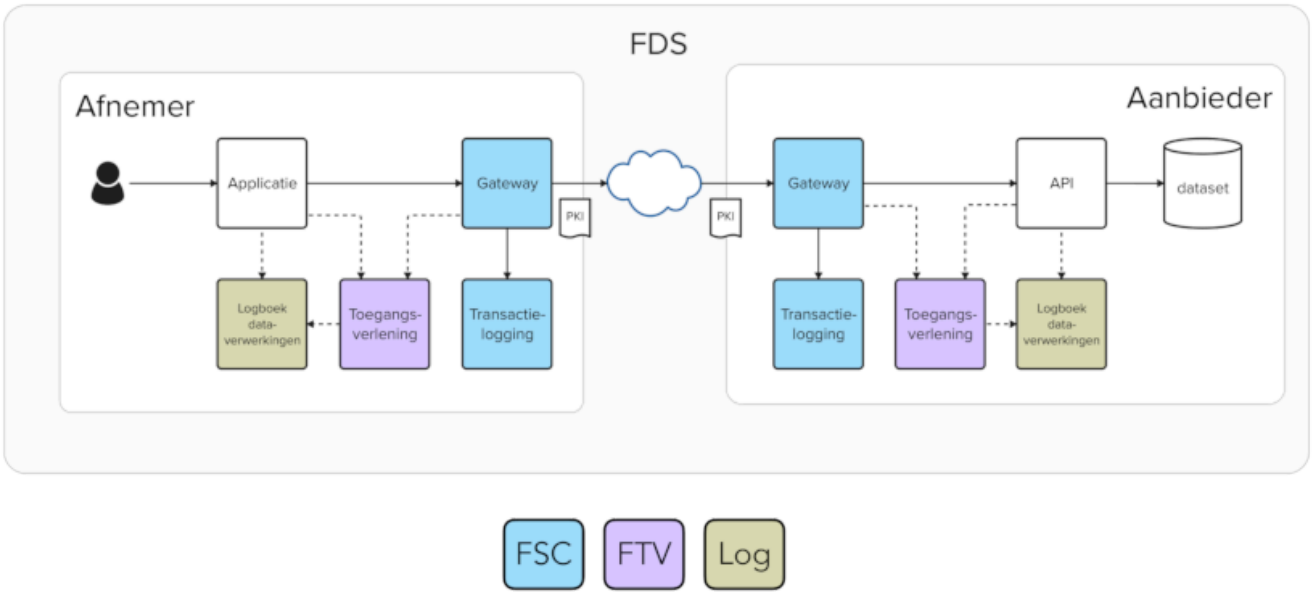
- BBN2 is het niveau dat volgens GEMMA geldt voor gegevensverwerkingen in de schuldhulpverlening.

Implicaties

- De BIO maatregelen moeten gericht zijn op het behalen van het beveiligingsniveau BBN2.

§ 2. Overzicht API stelsel

In de onderstaande figuur staan de componenten geschetst die in het API berichtenverkeer een rol spelen.



In deze figuur betekent:

FDS: Federatief Datastelsel (hier niet relevant, maar dit schema is daaraan ontleend en geeft aan dat DDAS past in een Federatief Datastelsel)

Afnemer: CBS

Aanbieder: de schuldhulpverlenende organisatie of de gegevensleverancier hiervan

PKI: Public Key Infrastructure - systeem voor het uitgeven en beheren van digitale certificaten

FSC: Federatieve Services Connectiviteit - standaard voor het leggen van koppelingen m.b.v. API's

FTV: Federatieve Toegangsverlening - een standaard voor het inrichten en beheren van gecontroleerde toegang tot gegevensdiensten in een stelsel

Log: Logging t.b.v. monitoring en verantwoording

Deze specificatie richt zich primair op de beschrijving van de API (rechtsboven in de figuur bij de aanbieder van gegevens), maar ook de andere componenten worden benoemd. Bent u enkele geïnteresseerd in de OpenAPI specificatie van de API? Deze staat onder het kopje "Berichten".

§ 3. Transportlaag

Het transport van de berichten verloopt volgens de FSC-standaard. De belangrijkste aspecten van deze standaard zijn:

- Dubbelzijdig TLS. NB: Dit vereist een certificaat dat door alle betrokken partijen vertrouwd wordt.
- Gebruik van PKIo certificaten voor authenticatie op basis van het Nederlandse profiel van OAuth. Deze zijn aan te vragen bij door Logius geautoriseerde aanbieders - er is een "services" certificaat nodig met EKU (Extended Key Usage) "TLS Web Client Authentication".
- Berichten lopen via FSC-componenten "outway gateway" van de afnemer (CBS) en "inway gateway" van de gegevensleverancier met de API.
- De "directory" van FSC waarin alle endpoints van de gegevensleveranciers staan wordt beheerd door RINIS.

- Geen gebruik van Diginetwerk - de betrokken organisaties zijn daar niet op aangesloten. Transport gaat via het “open” internet.

§ 4. Identificatie, Authenticatie en Autorisatie

Het bijhouden van de deelnemers in het DDAS-stelsel gebeurt door CBS in een directory die door FSC gebruikt wordt. Alle deelnemers gebruiken deze directory bij het uitwisselen van berichten.

§ 4.1 Identificatie

- Hoe worden de gegevensleveranciers geïdentificeerd? Als het mogelijk is wordt hiervoor het (sub)OIN van de gegevensleverancier gebruikt. Als de gegevensleverancier geen (sub)OIN heeft, dan moet een unieke identifier gekozen worden, waarmee ook het PKIo certificaat aangevraagd kan worden (vermoedelijk het KvK-nummer?).

§ 4.2 Authenticatie

- Systemen worden geauthenticeerd met behulp van het PKIo certificaat.

§ 4.3 Autorisatie

Er is voorlopig maar één service met een vaste set gegevens, waar maar één partij (CBS) toegang toe zal krijgen. Daarom is er geen autorisatie nodig, anders dan het verkrijgen van toegang tot de service. Partijen die toegang hebben tot de service zijn geautoriseerd om gegevens te bevragen. Deze autorisatie ligt vast in de directory van FSC, die door CBS beheerd wordt.

Als fijnmaziger autorisatie nodig is, dan bestaat er een voorkeur voor PBAC (Policy Base Authorisation Control). De autorisatie wordt dan bepaald op basis van beleidsregels, zoals “organisatie X krijgt toegang tot gegeven G als de organisatie overeenkomst O getekend heeft en het gegeven is vrijgegeven door autoriteit A”. Het is dan nog wel de vraag wie deze beleidsregels vaststelt en wie ze beheert.

§ 5. Signing en Versleuteling

§ 5.1 Signeren (Signing)

Alle berichten moeten ge-signed worden om de authenticiteit en onweerlegbaarheid van het berichtenverkeer te garanderen.

Signing gebeurt op basis van ADR-HTTP Message and payload signing with JAdES - zie "Uitgangspunten" voor de onderbouwing hiervoor. Het signeren van het bericht gebeurt met de privé sleutel van de verzender van het bericht, zodat de controle met de publieke sleutel van de verzender kan gebeuren en in principe iedereen de handtekening kan controleren. Iedere deelnemer van het DDAS-stelsel heeft dus een certificaat nodig voor het ondertekenen van de berichten. Dit moet een ander certificaat zijn dan welke voor het transport gebruikt wordt! Ook dit certificaat is een "services" certificaat, maar met EKU (Extended Key Usage) "Digital Signature".

5.2 Versleuteling (Encryptie)

Is versleuteling nodig? Er zijn vooralsnog geen routeervoorzieningen nodig berichten mogelijk gelezen kunnen worden, en het transport is dubbelzijdig versleuteld. Het transport loopt wel over het "open" internet.

Voorstel: Geen versleuteling.

Als versleuteling toch vereist wordt, dan versleuteling op basis van ADR-HTTP Payload encryption. De versleuteling gebeurt met de publieke sleutel van de ontvanger, zodat alleen de ontvanger het bericht kan ontsleutelen. De sleutel mag niet dezelfde zijn als die voor signing of TLS wordt gebruikt; er is dus een extra certificaat nodig voor versleutelen. Alleen de berichten met gevoelige (persoons)gegevens moeten versleuteld worden. Dit zijn de response-berichten van de gegevensleveranciers - in de request-berichten van CBS zitten geen gevoelige gegevens. Dit betekent dat er voor versleuteling één extra certificaat nodig is: bij CBS.

6. Berichten

De technische beschrijving van de API is het volgende OAS3-bestand beschreven.

```
{!../v0.1/DDAS-API_v0.1.1.yaml!}
```

Hiervan is ook een downloadbare versie van.

Hieronder worden de berichten die in het OAS-bestand technisch beschreven zijn, toegelicht.

6.1 Encoding

Conform de uitwisselspecificatie die voor de bestandsuitwisseling gebruikt wordt, is de encoding van de berichten UTF-8.

6.2 Vraagbericht (request)

Dit is het vraagbericht zoals dat door CBS naar de schuldhulpverlener gestuurd wordt. Alleen een POST request: alleen opvragen gegevens, geen mutaties. Bij GET zitten de parameters in de URL, waardoor mogelijk cache gegevens gebruikt worden, als de parameters niet wijzigen - daarom alleen een POST.

Voorstel voor parameters die meegestuurd kunnen worden (allemaal optioneel):

- Startdatum (date, default leeg - deelnemer bepaalt dan startdatum)
- Einddatum (date, default leeg - deelnemer bepaalt dan einddatum)
- Aanleverende_organisatie (string, default alle – alleen relevant als over meer dan 1 organisatie (gemeente/ schuldhulpverlener) gegevens aangeleverd worden)

Het bericht wordt met JAdES ondertekend met de private sleutel van de verzender van het vraagbericht.

6.3 Antwoordbericht (response)

Dit is het antwoordbericht van de gegevensbeheerder (systeem dat de bron beheert) met de gewenste gegevens in JSON formaat.

Ook dit bericht wordt ondertekend met JAdES met gebruik van de eigen private sleutel.

Als versleutelen nodig is (vooralsnog wordt ervan uitgegaan dat dit niet nodig is), wordt het bericht versleuteld conform ADR-HTTP Payload encryption met de publieke sleutel van de afnemer waar het antwoordbericht naartoe gaat (in dit geval altijd CBS). Of dit noodzakelijk is, is nog een punt van dicussie - vooralsnog wordt ervan uitgegaan dat dit niet nodig is. In de OAS3.1 specificatie is alleen signing opgenomen, geen versleuteling. Mocht versleutelen vereist zijn, dan wordt de API als volgt beschreven: OAS3.1 specificatie met versleuteling.

Payload is gebaseerd op uitwisselspecificatie!

Mogelijke responses:

- 200: bericht goed verwerkt (met versleutelde en gesigneerde payload)
- Foutberichten moeten nog bepaald worden - nu zijn 400 (ongeldig verzoek) en 401 (Ongeautoriseerd, OAuth2-token vereist) opgenomen

7. Niet functionele eisen

7.1 Beschikbaarheid

Niet kritische toepassing: geen hoge beschikbaarheid vereist.

Afstemmen met CBS: wanneer willen zij gegevens verzamelen? Dan zou de beschikbaarheid wat hoger moeten zijn. BV: tijdens kantooruren

7.2 Performance

Geen afhankelijkheden in het primaire proces: geen hoge performance vereist.

Wordt gebruik van cache toegestaan (volgens mij moet dat kunnen)? Onder welke voorwaarden?

7.3 Logging en Monitoring

Verantwoordelijkheid voor monitoring ligt bij partij die verantwoording hierover moet afleggen. Omdat er persoonsgegevens verwerkt worden, moet in elk geval rekening gehouden worden met de AVG. Daarom moet gelogd worden welke BSN's met wie uitgewisseld worden. Hierover moet ook gerapporteerd kunnen worden naar de betrokken burgers.

Vraag: Welke verantwoording verwacht het programma of SZW?

Voor gemeenten (suggestie):

- Aantal bevragingen naar datum en afzender (dat zou altijd CBS moeten zijn).
- Aantal en soort foute bevragingen.
- Aantal en soort meegestuurde parameters.
- Uitgewisselde BSN's met afnemer (altijd CBS?), zodat een burger inzicht kan krijgen in wie wanneer zijn gegevens heeft opgevraagd. NB: BSN's zijn persoonsgegevens. Als deze in de logging worden vastgelegd, moeten de privacy van die gegevens gegarandeerd worden. In de DPIA moet vastgelegd worden welke maatregelen hiervoor getroffen worden.

Voor CBS (suggestie):

- Aantal bevragingen naar datum en schuldhulpverlener.
- Aantal en soort (evt foutcodes) responses.

§ 8. Aanleverprotocol

Stappen bij het aanleveren van gegevens:

- CBS bevraagt de FSC directory bij RINIS om de endpoints van de gegevensleveranciers op te halen
- CBS roept via de FSC-outway de FSC-inway en daarmee de API van de gegevensleverancier aan (eventueel met parameters) met een requestbericht dat gesigneerd is met privé sleutel van CBS
- De gegevensleverancier controleert de signatuur met de publieke sleutel van CBS
- Indien OK, dan stuurt de gegevensleverancier de gegevens in het responsebericht dat gesigneerd is met eigen privé sleutel
- CBS controleert response technisch (signing, berichtformaat, viruscontrole)
- CBS controleert response functioneel/ inhoudelijk (relatie tussen velden, vreemde waarden, etc.)
- CBS stuurt een verwerkingsverslag ("op orde bericht") naar de gegevensleverancier *[nog ter discussie hoe dit het beste kan]*
- Indien OK, dan worden de gegevens bij CBS ingelezen in de database
- CBS loopt alle gerapporteerde trajecten af en combineert trajecten van dezelfde BSN bij dezelfde gemeente tot één “traject”
- CBS genereert de gewenste statistieken

NB: Als er bij deze stappen algoritmen gebruikt worden, moeten deze voldoen aan de Europese AI-verordening (definitieve tekst nog niet gevonden) en aangemeld worden bij het Algoritmeregister van de Nederlandse overheid.

§ 9. Aansluitprotocol

Iedere schuldhulpverleningsorganisatie of gemeente, eventueel via een gegevensleverancier (hierna: "deelnemer") die gegevens beschikbaar gaat stellen aan CBS, moet het aansluitprotocol doorlopen. Dit protocol valt onder

verantwoordelijkheid van het programma DDAS. Voor vragen hierover kan altijd contact opgenomen worden met *[contactadres]*.

Het protocol kan aangepast worden als hiervoor aanleiding is. Na aanpassingen wordt de meest recente versie met versienummer en versiedatum gepubliceerd op *[documentatiewebsite]*.

De stappen die de deelnemer moet doorlopen, zijn:

- De deelnemer meldt zich bij de stelselbeheerder (CBS of DDAS?) via het aanmeldformulier *[waar staat dit? wie beheert dit?]*, waarin in elk geval het volgende ingevuld:
    - Naam van de deelnemer + contactgegevens
    - Naam van de gegevensleverancier + contactgegevens
    - Endpoint waar de productiegegevens beschikbaar komen
    - Endpoint waar de testgegevens beschikbaar komen
    - Akkoord met de aansluitvoorwaarden*, waaronder de verwerkersovereenkomst met CBS?*
    - Eventuele verzoeken om de aansluiting tot stand te krijgen, zoals een gewenste publicatiedatum, specifieke testdata of specifieke beschikbaarheid
- *Indien PKIo certificaten niet mogelijk zijn: de stelselbeheerder (DDAS of CBS?) genereert een certificaat voor de TLS verbinding, signing en encryptie, en levert deze aan de deelnemer.*
- De deelnemer richt in de testomgeving de API, conform de AOS documentatie in. Voor de installatie van FSC komt een handleiding en een referentie implementatie beschikbaar.
- De deelnemer voert CBS op in de management module van FSC, om toegang te verlenen.
- CBS voert enkele bevragingen uit in de testomgeving en beoordeelt de kwaliteit van de gegevens. Op basis van de bevindingen wordt de API aangepast.
- Indien er geen blokkerende bevindingen zijn, krijgt de deelnemer vrijgave van de stelselbeheer (DDAS?) en wordt de API in de productieomgeving ingericht en beschikbaar gesteld.
- CBS laat de deelnemer opvoeren in de FSC management module van RINIS, zodat de API beschikbaar komt in het stelsel en bevraagd kan worden bij het ophalen van alle gegevens.

Ten behoeve van de testen stelt DDAS een set testgegevens beschikbaar *[wie maakt deze set? waar komt dit te staan?]*.

Voor ondersteuning bij de aansluiting is een referentie implementatie en documentatie beschikbaar *[waar?]* en kan contact opgenomen worden met *[contactadres]*. Als er bij de aansluiting bevindingen zijn, die niet door de deelnemer opgelost kunnen worden, kan een wijzigingsverzoek ingediend worden.

§ 10. Beheer van de specificatie

De koppelvlakspecificatie is onderhevig aan wijzigingen: de technologie ontwikkelt zich, er zijn mogelijk andere gegevens nodig, de samenwerking tussen de betrokken partijen kan wijzigen, etc. Om deze wijzigingen op een betrouwbare en juiste manier te verwerken in de specificatie, is een wijzigingsproces ingericht. Dit wijzigingsproces valt onder verantwoordelijkheid van de stuurgroep DDAS en wordt uitgevoerd door het programma DDAS, zolang het programma DDAS actief is. Daarna wordt het overgedragen aan een nog aan te wijzen organisatie. Voor het beoordelen van wijzigingsverzoeken wordt een beheeroverleg samengesteld, met afgevaardigden van de betrokken partijen, onder

voorzitterschap van het programma DDAS. Dit beheeroverleg komt periodiek bijeen om wijzigingsverzoeken te beoordelen en eventueel verder uit te werken.

Het streven is om maximaal eenmaal per jaar een nieuw release van de koppelvlakspecificatie uit te brengen.

§ 10.1 Indienen wijzigingsverzoek

Wijzigingsverzoeken worden verzameld via [nog in te vullen]. Alle betrokken partijen mogen wijzigingsverzoeken indienen. Er is geen template voor het indienen van een wijzigingsverzoek, maar het verzoek moet in elk geval de volgende informatie bevatten:

- Indiener (inclusief contactgegevens)
- Datum indienen
- Beschrijving gewenste wijziging (bondig, maar voldoende specifiek om in te kunnen schatten wat de impact is)
- Onderbouwing/ aanleiding gewenste wijziging
- Prioriteit volgens de indiener (hoe snel moet de wijziging doorgevoerd worden)

Als het aantal wijzigingsverzoeken groot wordt of de afhandeling daarvan complex, dan wordt een systeem gebruikt om een en ander in te administreren.

Dit systeem moet zo openbaar mogelijk zijn, om zo transparant mogelijk te zijn over de afhandeling van verzoeken en om te voorkomen dat dezelfde wijzigingsverzoeken meerdere malen ingediend worden.

§ 10.2 Afhandelen wijzigingsverzoek

Het wijzigingsverzoek wordt door het programma DDAS geanalyseerd, waarbij vastgesteld wordt welke onderdelen van de specificatie geraakt worden en wat de geschatte impact is op de specificatie, de techniek, de processen en de betrokken partijen. Tevens wordt ingeschat wat de randvoorwaarden, kosten en doorlooptijd van de gewenste wijziging zouden zijn. Dit leidt tot een voorstel voor de verdere afhandeling: of, hoe en wanneer dit wijzigingsverzoek doorgevoerd wordt.

Het wijzigingsverzoek met de analyse van het programma DDAS worden besproken in het (nog in te richten) beheeroverleg DDAS. Als alle betrokken partijen akkoord gaan met de voorgestelde afhandeling, wordt deze afhandeling gevolgd (d.w.z. inplannen voor een release, via noodprocedure eerder doorvoeren, of afwijzen van het verzoek).

§ 10.3 Releaseproces

Wijzigingen die doorgevoerd moeten worden, worden zoveel mogelijk via een release in productie gebracht. Het streven is om maximaal eenmaal per jaar een release door te voeren. De stappen die hiervoor doorlopen worden zijn:

- Vaststellen scope van de release door de stuurgroep DDAS, op basis van advies van beheeroverleg [6 maanden voor productiedatum]
- Publiceren aangepaste specificatie door programma DDAS [5 maanden voor productiedatum]

- Doorvoeren noodzakelijke wijzigingen in de testomgeving door deelnemers (gegevensleveranciers en CBS) [tot 1 maand voor productiedatum]
- Testen nieuwe release in testomgeving [in laatste maand voor productiedatum]
- Livegang nieuwe release

§ 10.4 Releasenummering

Ieder release wordt aangeduid met een releasenummer. Deze krijgt de vorm X.Y, waarbij X het "major" nummer is en Y het "minor" nummer. Voor testreleases kan een derde nummer toegevoegd worden; het zogenaamde "patch" nummer. In de productieomgeving wordt geen patch nummer gebruikt.

Als een release via het reguliere releaseproces naar productie gaat, dan krijgt deze een nieuw major nummer en het minor nummer 0 (bv. "1.0"). Als er via de noodprocedure een release doorgevoerd wordt, dan blijft het major nummer hetzelfde, maar wordt het minor nummer opgehoogd (bv. "1.1").

§ 10.5 Vrijgaveprocedure en afwijkingsverzoeken

Er is geen "vrijgave" van deelnemers voor een release nodig. Als de specificatie complexer wordt kan de stuurgroep DDAS besluiten om een vrijgaveprocedure in te richten. De deelnemer moet dan aan de hand van een set testscenario's aantonen te voldoen aan de nieuwe specificaties. Als dit succesvol is, dan krijgt de deelnemer vrijgave voor de nieuwe release. Als dit niet succesvol is, dan kan de deelnemer een afwijkingsverzoek indienen bij het programma DDAS en toch gegevens blijven aanbieden. Een afwijkingsverzoek wordt alleen geaccepteerd als dit de rapporten van CBS niet compromitteert. In het afwijkingsverzoek wordt altijd aangegeven hoe lang de afwijking geldig mag blijven.

§ 10.6 Noodprocedure

Het kan gebeuren dat een wijziging niet kan wachten op een gepland release, maar sneller doorgevoerd moet worden. De stuurgoep DDAS kan dan op advies van het beheeroverleg, een noodprocedure aanroepen.

Het beheeroverleg adviseert de stuurgroep welke stappen genomen moeten worden en in welk tempo deze doorlopen moeten worden. Als de stuurgroep hiermee akkoord gaat, voert het programma DDAS de regie op de uitvoering van de stappen.

De release die hiermee ontstaat krijgt geen nieuw "major" versienummer, maar een nieuw "minor" nummer (zie ook "releasenummering").

§ 10.7 Escalatie

Als de partijen het niet eens worden, wordt het verzoek geëscaleerd naar de stuurgroep DDAS. Als het behandelen van het verzoek niet kan wachten tot het eerstvolgende overleg van de stuurgroep, worden de stuurgroepleden schriftelijk om hun oordeel gevraagd.

↥