DDAS API Koppelvlakspecificatie

Samenvatting

Dit document bevat de koppelvlakspecificatie voor het de API waarmee schuldhulporganisaties gegevens beschikbaarstellen aan het CBS. Dit is een product van het [programma DDAS] (https://www.divosa.nl/projecten/data-delen-over-armoede-en-schulden). Het [informatie- en uitwisselmodel] (https://brienen.github.io/ddas/latest/) dat gebruikt wordt, is niet volledig opgenomen in deze specificatie. De OAS beschrijving van de API wordt binnenkort gepubliceerd.

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.

Inhoudsopgave

1. Inleiding

Het einddoel van het project “Datadelen op Armoede en Schulden” is om de betrokken partners in het domein gezamenlijk regie te laten voeren op de informatievoorziening over schulden en armoede om op die manier hoge kwaliteit en beschikbaarheid van data te garanderen. Om dat te bereiken gaan we de uitvraag van schuldhulpdata bij gemeenten sterk vereenvoudigen, verbeteren en borgen. Eén van de middelen om de uitvraag te verbeteren is het ontwikkelen van een API-structuur en een API-werkwijze. Deze koppelvlakspecificatie geeft invulling aan de API-structuur en -werkwijze. De koppelvlakspecificatie beschrijft de wijze waarop de gewenste gegevens op een veilige en robuuste manier beschikbaar gesteld kunnen worden. Deze specificatie gaat niet specifiek in op de inhoud en betekenis van de gewenste gegevens. Hiervoor wordt verwezen naar het informatiemodel []. De technische uitwerking van de berichten die in deze koppelvlakspecificatie beschreven worden is in OAS3 formaat te vinden … [publiceren OAS specificaties op Github?] NB: de huidige versie bevat de vragen, verzamelde antwoorden en voorstellen waar een keuze in gemaakt moet worden. Met deze keuzes wordt het document in volgende versies uitgewerkt. Deze specificatie wordt, na afstemming met de betrokken partijen, vastgesteld door de stuurgroep. Na vaststelling kunnen wijzigingsverzoeken bij het programma DDAS ingediend worden. Indien nodig volgt dan een aangepaste versie, die opnieuw door de stuurgroep vastgesteld wordt.

§ 2. Uitgangpunten

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
- FSC

De volgende keuzes zijn gemaakt:

- Gebruik Digikoppeling REST-API standaard
- JSON formaat voor berichten
- Gebruik Diginetwerk voor transport
- Gebruik PKIo certificaten
- Gebruik JWS voor signen
- Gebruik JWE voor encryptie
- Beveiligingsniveau BBN2 (zou uit DPIA moeten volgen)

§ 3. Transportlaag

Hoe ziet de technische uitwisseling van berichten eruit.

Vragen:

- Gebruik van Diginetwerk? Kunnen alle organisaties die gegevens gaan leveren hierop aansluiten? Wordt waarschijnlijk niet mogelijk... Dan via “open” internet: vereist mogelijk extra maatregelen, zoals versleuteling van de gegevens. Dit hangt af van de DPIA.
- Dubbelzijdig TLS (wordt voorgeschreven in Digikoppeling en FSC standaard) 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? Het is de vraag of alle partijen een PKIo certificaat mogen aanvragen. Als dit niet mogelijk is, moet een “trust anchor” gevonden worden: de autoriteit die certificaten kan uitgeven, die door alle betrokken partijen vertrouwd worden.

§ 4. Identificatie, Authenticatie en Autorisatie

Hoe worden de schuldhulpverleners (gegevensleveranciers) geïdentificeerd? (o.b.v. (sub)OIN?) Als niet alle betrokken partijen een (sub)OIN kunnen krijgen, moet een systematiek gevonden worden om alle partijen uniek te kunnen identificeren.

Hoe worden systemen geauthenticeerd? (obv PKIo certificaten? Als dat niet kan: wie wordt de “Trust Anchor” – de autoriteit die door alle partijen vertrouwd wordt?)

Autorisatie lijkt niet heel spannend: er zal waarschijnlijk maar één service komen met een vaste set gegevens, waar maar één partij (CBS) toegang toe zal krijgen. 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”. Dan is de vraag wie deze beleidsregels vaststelt en wie ze beheert.

§ 5. Signing en Versleuteling

NB: De Digikoppeling standaard voor REST-API heeft (nog) geen standaard voor signing en encryptie vastgesteld. Daarom voorstel om JWT te gebruiken en dus eerst een JWT aan te vragen, die daarna bij het request wordt meegestuurd. Eventueel kunnen hierbij protocollen van de FSC standaard toegepast worden.

§ 5.1 Signing

Voorstel: Signing op basis van JWS in een JWT conform de FSC standaard.

§ 5.2 Versleuteling (Encryptie)

Is versleuteling nodig? (zou uit DPIA moeten komen – ik vermoed dat het nodig is)

Voorstel: Versleuteling op basis van JWE in een JWT met PKIo certificaten. NB: ook hier geldt dat als niet alle betrokken partijen PKIo certificaten kunnen aanvragen, er een Trust Anchor nodig is die vertrouwde certificaten kan uitgeven.

§ 6. Berichten

§ 6.1 Vraagbericht (request)

Request zoals dat door CBS naar de schuldhulpverlener gestuurd wordt. Alleen een GET en/ of 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.

NB: Met een JWT voor authenticatie, signen en versleutelen (als versleutelen nodig is – met een BSN in het bericht zou dat waarschijnlijk moeten). Mogelijk kan dit afgevangen worden door het FSC-concept van inward- en outward-services?

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

- Startdatum (default vandaag)
- Einddatum (default vandaag)
- Gemeente (default alle – alleen relevant als over meer dan 1 gemeente gegevens aangeleverd worden)
- BSN? (of ander gegeven waarmee een inwoner geïdentificeerd kan worden – default alle)
- SHV-traject? (default alle)

Technische uitwerking in OAS3 (YAML/ JSON bestand op Github?)

6.2 Antwoordbericht (response)

Response van de schuldhulpverlener met de gewenste gegevens in JSON formaat.

Als versleutelen nodig is, in een JWE vorm (eventueel gezipt, versleuteld in een token).

Payload zoals gedefinieerd door Arjen!

Responses: opnemen in OAS3 beschrijving. Bv:

- 200: bericht goed verwerkt (met payload)
- Welke foutberichten? (FSC standaard volgen?)

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 Monitoring

Verantwoordelijkheid voor monitoring ligt bij partij die verantwoording hierover moet afleggen. Welke verantwoording verwacht het programma of SZW?

Voor gemeenten (suggestie):

- Aantal bevragingen naar datum en afzender (altijd CBS?)
- Aantal en soort foute bevragingen
- Aantal en soort meegestuurde parameters

Voor CBS:

- Aantal bevragingen naar datum en schuldhulpverlener
- Aantal en soort responses

8. Aanleverprotocol

Stappen bij het aanleveren van gegevens:

- CBS roept systeem van schuldhulpverlener (gegevensleverancier) aan om JWT voor signing en encryptie te krijgen
- CBS roept API van de gegevensleverancier aan (eventueel met parameters)
- CBS controleert response technisch (signing, viruscontrole, berichtformaat)
- CBS controleert response functioneel (verplichte velden, vreemde waarden, etc.)
- CBS stuurt een verwerkingsverslag naar de gegevensleverancier
- Indien OK, dan worden de gegevens ingelezen in de database
- CBS loopt alle gerapporteerde trajecten af en combineert trajecten van dezelfde BSN tot één “traject”
- Bij het combineren wordt de volledigheid en kwaliteit van de gegevens gecontroleerd – op basis daarvan krijgt het traject een "betrouwbaarheidsindicator""

- CBS genereert de gewenste rapporten

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 (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 [yaml-bestand, nog toe te voegen] 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 of CBS?) en wordt de API in de productieomgeving ingericht en beschikbaar gesteld.
-
- CBS voert de deelnemer op in de management module van FSC, zodat de API bevraagd wordt 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.