VNG Realisatie Standaard - In Ontwikkeling versie

DDAS API Koppelvlakspecificatie 2026.01

Koppelvlakspecificatie voor het beschikbaarstellen van DDAS-gegevens aan het CBS

VNG Realisatie Standaard
In Ontwikkeling versie 14 januari 2026

Deze versie:
https://vng-realisatie.github.io/publicatie/hl/respec-template/2026.01

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.

Naast de uitgangspunten en de technische specificatie bevat dit document een beschrijving van de niet-functionele eisen (beschikbaarheid, performance).

De huidige versie is nog in ontwikkeling. De verwachting is dat de definitieve versie begin april 2026 beschikbaar komt. De uitgangspunten en de daaruit volgende keuzes zullen grotendeels gelijk blijven, maar specifieke invulling kan nog veranderen. Daarom kunnen er 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 zijn.
- De API waarmee gegevens beschikbaar gesteld worden, kan hergebruikt worden voor andere toepassingen.
- Dit patroon is besproken in de stuurgroep van 17 maart 2025 en als voorkeurspatroon geaccepteerd (rekening houdend met de risico's en maatregelen die in de besproken beslisnotitie zijn meegegeven).

Implicaties

- Alle gegevensleveranciers moeten een API als service beschikbaar stellen waar de DDAS-gegevens opgevraagd kunnen worden.
- De service moet voldoende beschikbaar zijn om CBS op de afgesproken momenten te faciliteren.
- Er is geen centrale routeervoorziening of gegevensopslag nodig. Wel is een centrale "directory" nodig waar de services gepubliceerd worden, waarmee CBS de gegevens kan ophalen. Er moet een keuze gemaakt worden waar deze directory belegd wordt.

Gebruik Digikoppeling REST profiel

Rationale

- De Digikoppeling standaard is de overheidsstandaard voor gegevensuitwisseling.
- Het REST 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.
- Het REST profiel stelt de FSC standaard als verplicht voor de inrichting van het koppelvlak - hier moet dus ook aan voldaan worden.

Gebruik JAdES voor signen

Rationale

- Het REST profiel van Digikopeling stelt JAdES verplicht als de inhoud of de header van een bericht gesigned wordt.
- 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).

Berichten worden niet versleuteld*

Rationale

- Omdat het berichtenverkeer rechtstreeks tussen aanbieder en afnemer verloopt, is een "Man-in-the-Middle" aanval niet waarschijnlijk.
- De transportlaag wordt "end-to-end" versleuteld. Dit levert voldoende zekerheid dat de gegevens niet door ongeautoriseerde partijen gelezen kunnen worden.

Implicaties

- Berichten hoeven niet versleuteld en ontsleuteld te worden.

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. Deze componenten zijn onder de naam OpenFSC als Open Source beschikbaar.
- 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

- Er is een centrale directory nodig waar gegevensleveranciers hun services kunnen publiceren en waar met CBS een contract afgesloten kan worden.
- 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. Vooralsnog is dit niet nodig en wordt de algemene omgeving van RINIS gebruikt.

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 de stelselbeheerder (gedurende het programma is dit het programma DDAS).
- Voor het ophalen van de gegevens, moet CBS de directory van RINIS bevragen om een contract af te sluiten met de leverancier van gegevens. Daarmee krijgt CBS toegang tot de service die de gegevens ontsluit.

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 RINIS worden alleen vertrouwde endpoints aangeroepen en krijgen alleen vertrouwde consumers (in dit geval enkel CBS) toegang tot de services.

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 en waarvoor een contract is afgesloten tussen CBS en gegevensleverancier, 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.

Beveiligingsniveau BBN2

Rationale

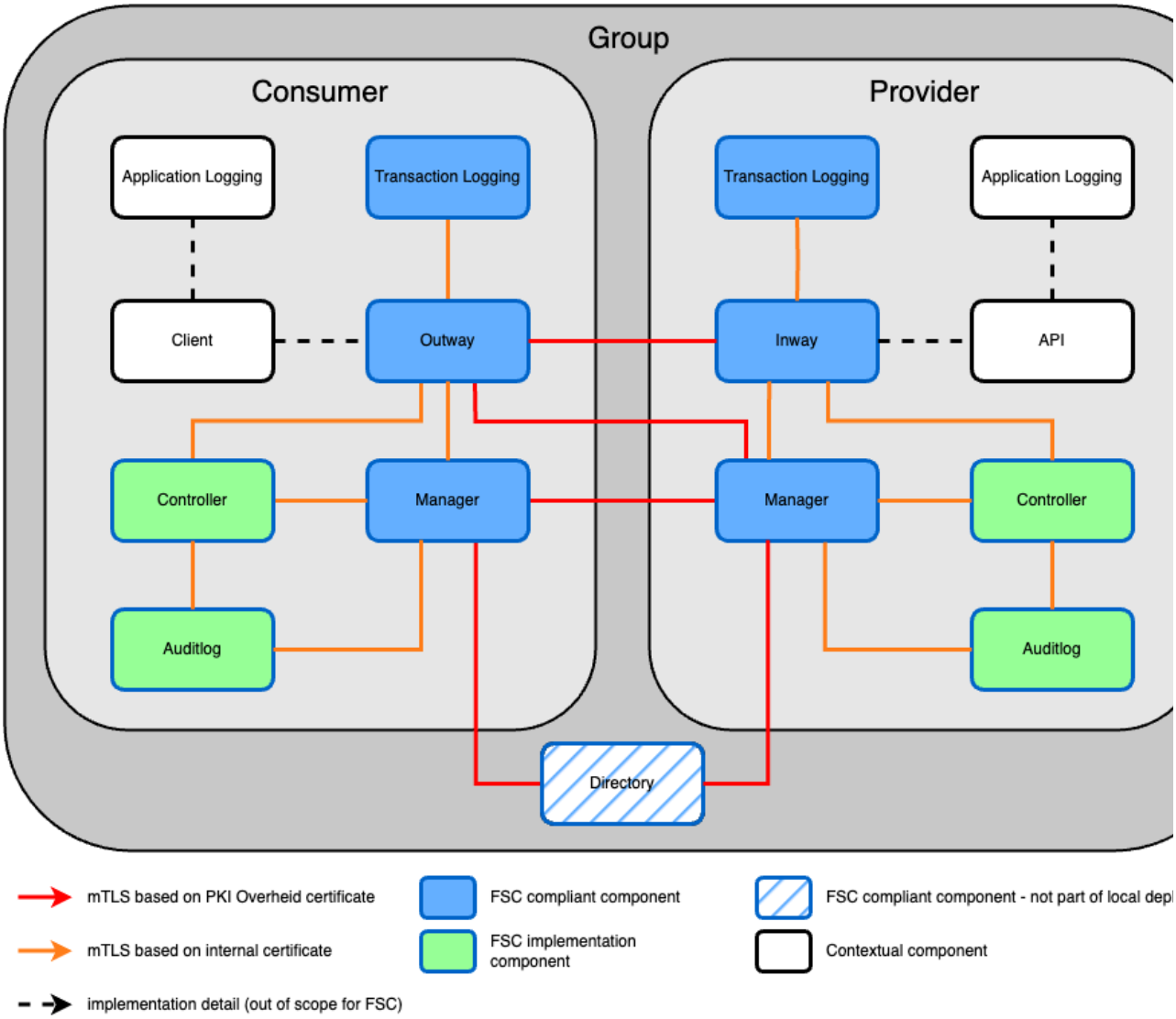
- BBN2 is het niveau dat volgens GEMMA geldt voor gegevensverwerkingen in de schuldhulpverlening.

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 is:

- Consumer: de vragende partij - hier is dat CBS
- Provider: de leverende partij - hier is dat de schuldhulpverlenende organisatie of de gegevensleverancier hiervan
- De "directory" waar alle services (API's) gepubliceerd worden, wordt door RINIS beheerd

Deze specificatie richt zich op de inrichting van alle componenten van dit koppelvlak. Bent u enkel 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. Deze zijn aan te vragen bij door Logius geautoriseerde aanbieders.
- De autorisatie van verbindingen wordt gedaan met een client credentials flow die voldoet aan het Nederlandse profiel van OAuth.
- 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 services 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.

De inrichting van de transportlaag volgt de stappen die in de FSC standaard genoemd worden:

- Ontwerp, bouw en implementatie van de API die beschikbaar gesteld gaat worden, conform de OAS3 beschrijving.
- Keuze inrichting en implementatie van FSC componenten in de eigen omgeving. Hiervoor kan gebruik gemaakt worden van de documentatie en de referentie-implementatie van FSC.
- Aanmelden bij Demo groep van RINIS en testen verbinding en FSC componenten. NB: hiervoor zijn geen PKIo certificaten nodig.
- Aanmelden bij Acceptatie groep van RINIS en publiceren van acceptatie versie van de service. NB: hiervoor zijn geen PKIo certificaten nodig.
- Testen van verbinding en service in overleg met CBS. In deze stap kan de API ook inhoudelijk getest worden: worden de juiste gegevens in het juiste formaat beschikbaar gesteld?
- Als de testen het gewenste resultaat leveren, aanmelden bij Productie groep van RINIS. NB: hiervoor is een PKIo certificaat nodig.
- Publiceren van de productieversie van de service en afsluiten van een contract met de consumer (CBS).

§ 4. Identificatie, Authenticatie en Autorisatie

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

§ 4.1 Identificatie

- Identificatie gebeurt op basis van het (sub)OIN van de deelnemer. Dit (sub)OIN wordt bij PKIo certificaten geplaatst in het SerialNumber veld van het Subject. Als de deelnemer geen (sub)OIN heeft, dan wordt het handelregisternummer hiervoor gebruikt.

§ 4.2 Authenticatie

- Systemen worden geauthenticeerd met behulp van het PKIo certificaat.

§ 4.3 Autorisatie

De autorisatie voor toegang wordt vastgelegd in een FSC Contract tussen aanbieder en afnemer. Deze liggen vast in de FSC Manager van de betrokken deelnemers. Er is voorlopig maar één service met een vaste set gegevens, waar maar één partij (CBS) toegang toe zal krijgen. Daarom is er geen fijnmazige autorisatie nodig: partijen die toegang hebben tot de service zijn geautoriseerd om gegevens te bevragen.

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”. Deze regels worden centraal beheerd, zodat alle partijen de regels op dezelfde manier en met dezelfde betekenis hanteren.

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". Er is gekozen voor het gebruik van PKIo certificaten - zie "Uitgangspunten" voor de onderbouwing hiervan.

5.2 Versleuteling (Encryptie)

De inhoud van de berichten wordt niet versleuteld. Zie "Uitgangspunten" voor de onderbouwing hiervan.

6. Berichten

6.1 Schuldhulpverleningsgegevens

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

```
{!../v0.1/DDAS-SHV_v0.1.1.yaml!}
```

Hiervan is ook een downloadbare versie van.

6.2 Vroegsignaleringsgegevens

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

```
{!../v0.1/DDAS-VS_v0.1.1.yaml!}
```

Hiervan is ook een downloadbare versie van.

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

6.3 Encoding

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

6.4 Vraagbericht (request)

Dit is het vraagbericht zoals dat door CBS via de "Outway" naar de "Inway" van de schuldhulpverlener gestuurd wordt. Dit is een POST request waarbij alleen gegevens opgevraagd worden. Er worden geen GET requests gebruikt, omdat hierbij de parameters in de URL zitten en mogelijk cache gegevens gebruikt worden, als de parameters niet wijzigen.

Parameters die meegestuurd kunnen worden (allemaal optioneel):

- Startdatum (date, default leeg - schuldhulpverlener bepaalt dan startdatum)
- Einddatum (date, default leeg - schuldhulpverlener 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 - in dit geval CBS.

6.5 Antwoordbericht (response)

Dit is het antwoordbericht van de gegevensbeheerder (systeem dat de bron beheert) met de gewenste gegevens in JSON formaat. De payload is gebaseerd op het uitwisselformaat zoals dat is beschreven voor schuldhulpgegevens en vroegsignaleringsgegevens.

Ook dit bericht wordt ondertekend met JAdES met gebruik van de eigen private sleutel. Versleutelen van de payload is niet nodig.

Mogelijke responses:

- 200: bericht goed verwerkt (met versleutelde en gesigneerde payload)
- Foutberichten conform de FSC standaard:
  - Gegenereerd door de FSC Manager
  - Gegenereerd door de gekozen methode van FSC
  - Gegenereerd door de de FSC Inway

7. Niet functionele eisen

Dit onderwerp vraagt nog verdere uitwerking!

7.1 Beschikbaarheid

De toepassing is niet kritisch: er is geen hoge beschikbaarheid vereist. De services moeten beschikbaar zijn op de momenten dat CBS de gegevens verzameld. Hierover moeten nog afspraken gemaakt worden.

7.2 Performance

De berichtenuitwisseling is synchroon. De API moet daarom binnen de "time-out" tijd reageren op een request. Er is nog geen afspraak over de maximale response tijd die geaccepteerd wordt.

Om belasting van de productiesystemen te beperken mag een cache gebruikt worden, onder de volgende voorwaarden:

- De cache wordt minimaal dagelijks ververst.
- De integriteit van de gegevens in de cache kan gegarandeerd worden. De gegevensleverancier bepaalt zelf hoe deze garantie gegeven kan worden (bijvoorbeeld met controles, checksums, logging of andere maatregelen).

§ 7.3 Logging en Monitoring

Verantwoordelijkheid voor monitoring ligt bij partij die verantwoording hierover moet afleggen.

FSC vereist dat er transactielogging bijgehouden wordt. Hiervoor wordt de logging module van OpenFSC gebruikt. Deze vorm van logging bevat geen persoonsgegevens en vereist daarom geen specifieke privacy maatregelen.

Bij de logging van de vragende en leverende systemen, moet er rekening gehouden worden met de AVG als persoonsgegevens (zoals het BSN) gelogd worden. De DPIA heeft uitgewezen dat de uitgewisselde BSN's niet individueel gelogd hoeven te worden om te voldoen aan het inzagerecht (een algemene vermelding dat schuldhulpverleningsgegevens aan CBS beschikbaar gesteld worden, is voldoende). Dit wordt daarom afgeraden - logging met individuele BSN's vormen immers een nieuwe verwerking met daaraan gekoppelde risico's.

↥