Reactie op consultatie "ZORG-AB"

Aan: Informatieberaad Zorg
Namens: Stichting Nuts

In het Nuts initiatief wordt door softwareleveranciers in de zorg preconcurrentieel samengewerkt aan open standaarden waarmee we de zorg vooruit helpen. Samen ontwikkelen we een robuust netwerk voor gegevensuitwisseling in de zorg, van ons allemaal en voor ons allemaal. Dat doen we aan de hand van het Nuts manifest, dat in acht punten beschrijft hoe wij met elkaar wensen samen te werken.

We zullen in deze reactie de voorgestelde adresseringsvoorziening ZORG-AB naast dit manifest leggen. Daarbij zullen we uiteenzetten wat voor problemen één centraal systeem volgens ons met zich meebrengt, bespreken we de risico's van het ontwerp voor integriteit en vertrouwelijkheid en zullen we ook schetsen hoe wij zelf de toekomst van adressering voor ons zien.

"Zorgadresinformatie moet vrij toegankelijk zijn"

Om te beginnen: het doet ons deugd te zien dat er op een aantal punten overeenstemming lijkt te zijn tussen de voorgestelde voorziening en het Nuts manifest. In §3.2.c van het document *Opname van ZORG-AB als bouwsteen in het duurzaam informatiestelsel* (hierna: het voorstel) kunnen we lezen:

> ***Zorgadresinformatie moet vrij toegankelijk zijn**. De zorgmarkt moet zich kunnen richten op haar kerncompetentie, waarbij basisinformatie die kerncompetenties moet ondersteunen.*

Wij delen deze mening met de indieners. In punt vijf uit ons manifest beschrijven we dat toetreden tot ons netwerk van zorg-ICT leveranciers **frictieloos** moet zijn. Daaruit volgt dat systemen elkaar makkelijk en snel moeten kunnen vinden, en technische adressen dus vrij toegankelijk moeten zijn.

> **5. Open standaarden**
> ***Wij geloven dat toetreden tot dat netwerk frictieloos moet zijn.** De gezamenlijke communicatiestructuur moet open en gestandaardiseerd zijn en er mogen geen (licentie)kosten verbonden zijn aan het gebruik. [...]*

Ook maakt de bijgeleverde implementatiehandleiding van ZORG-AB heel duidelijk dat de aansluiting op de voorziening geschiedt op basis van **open standaarden**. Onze complimenten voor de kwaliteit van deze handleiding en het gebruik van OpenAPI specificaties voor de verschillende *endpoints*.

In het algemeen kunnen we stellen dat ook stichting Nuts en het samenwerkingsverband Centrale Voorzieningen (dat in 2019 is opgegaan in Nuts) het thema "adressering" als gemeenschappelijke voorziening, los van een specifieke use-case of zorg-niche, hebben **geagendeerd** als katalysator van gegevensuitwisseling in de Nederlandse zorg. Hoewel we tegenwoordig liever spreken over een "register", waarover later meer. Een dergelijk systeem opzichzelfstaand ontwerpen kan dus zeker op onze bijval rekenen.

Echter, wanneer we kijken naar de specifieke invulling die in het voorstel wordt gegeven aan die adresseringsvoorziening en het ontwerp dat daarbij wordt gehanteerd, dan zien we op verschillende aspecten daarvan overwegende bezwaren die we hieronder toelichten en beargumenteren.

Intenties en definities

Laten we vooraan beginnen, met de scope van ZORG-AB. Als we het hebben over adresinformatie, gaat het dan over gevelnamen, over adressen van vestigingen, over namen van behandelaren, over KvK registraties, over BIG nummers, over AGB nummers, over telefoon- of faxnummers, over e-mailadressen of zorgmailadressen, over URA-nummers, over technische endpoints en IP adressen van systemen, over cryptografische sleutels, of over nog iets anders? Gaat het over zorginstellingen, fysieke vestigingen, rechtspersonen of natuurlijke personen? Wat is eigenlijk, in de ogen van de indieners, **allemaal adresinformatie**?

In dit voorstel lijkt het over **al** die zaken te gaan, en daarmee verliest het wat ons betreft haar kracht. Een goed hulpmiddel is nauwkeurig en precies, en volledig geoptimaliseerd voor haar taak.

Dit is ook waarom wij bij Nuts tegenwoordig niet meer spreken over het thema “adressering” maar het thema “register”. Een register is wat ons betreft simpel, exact en heel praktisch: je zoekt een zorginstelling op gevelnaam op en je vindt technische endpoints en cryptografische sleutels. Allemaal cryptografisch ondertekend. En verder niets. Immers, als ik het telefoonnummer van die instelling wil weten dan kan ik dat vervolgens bij één van die endpoints opvragen. Dat hoeft helemaal niet centraal opgeslagen te staan als mijn computersysteem in staat is om dat rechtstreeks aan het computersysteem van de ander te vragen. Data bij de bron; dan is het **betrouwbaar en actueel**. Het register is daarmee beperkt tot *service discovery* die garanties over betrouwbaarheid geeft.

Doordat de scope van ZORG-AB veel breder lijkt en niet duidelijk is geformuleerd kunnen we ook heel moeilijk beoordelen of het voorgestelde model **toereikend** is voor het doel, of dat het dat doel ver voorbij schiet. We kunnen ook moeilijk voorspellen welke **uitbreidingen** van ZORG-AB er in de toekomst nodig zullen zijn en hoe kostbaar of hoe eenvoudig die zullen zijn. Maar dat er uitbreidingen nodig zullen zijn lijkt evident, juist door de gekozen aanpak om alle gegevens over een zorginstelling op één plaats te willen verzamelen.

Alles op één plek

We lezen in §3.1.o van het voorstel een aanname die we eigenlijk niet onderbouwd zien:

> ***Landelijk:***
> - *Een plek waar alle benodigde contactinformatie en noodzakelijke technische informatie wordt samengebracht, beheerd en gefaciliteerd. Centrale regie, waardoor de vertrouwelijkheid (geringe kans op onjuist adres) en integriteit (het beheer van de contactgegevens is ingeregeld) bij elke uitwisseling van medische gegevens beter te garanderen is.*

Zoals eerder geschreven geloven wij in het principe van data bij de bron, en zien we niet hoe de vertrouwelijkheid en integriteit van gegevens beter gegarandeerd worden door centrale regie. Integendeel: de vertrouwelijkheid en integriteit van de communicatie lijden eronder dat er een derde partij

tussen staat die **vertrouwd** moet worden dat de contactgegevens juist zijn zonder enige vorm van echtheidskenmerken. Op dit punt zullen we terugkomen in het hoofdstuk *Privacy & Security*.

Bij Nuts geloven we in de kracht van een gedistribueerd netwerk. Punt vier uit ons manifest:

> **4. Gedistribueerd netwerk**
> *Wij geloven in een gedistribueerd model van communicatie, vergelijkbaar met het Internet. Wij willen niet investeren in een netwerktechnologie met **één leverancier**, of één partij die direct of indirect alle gezondheidsdata van Nederland beheert. We willen een robuust netwerk van iedereen en voor iedereen, zonder **central point of failure** of **monopolist**.*

Het eerder beschreven Nuts register waar wij aan werken is daarom niet een centraal opgezette dienst die wordt beheerd door één partij, maar een **federatief systeem** waar elke leverancier die het gebruikt ook aan meedoet. Het vertrouwen in dat systeem ligt in de cryptografische ondertekening van de gegevens, niet in het beheer van toegang tot het systeem of de processen die daaromheen worden opgetuigd.

In het voorstel van ZORG-AB worden dit soort decentrale oplossingen op twee plekken benoemd in de context van de DIZRA. In §3.7.a:

> ***Federatieve samenwerking***
> *Feitelijk brengt ZORG-AB registers samen die anders per bron moeten worden geraadpleegd. ZORG-AB brengt een gekoppelde dataset van meerdere registers bij elkaar, zodat bijvoorbeeld een URA ook de koppeling naar meerdere AGB-codes bevat en vice versa. In de doorontwikkeling wordt rekening gehouden met de koppeling van meerdere adresvoorzieningen binnen een zorgadresinformatiestelsel.*

En in §3.11.b:

> *Bij de ontwikkeling van ZORG-AB wordt rekening gehouden met DIZRA (zie ook bijlage 3), waardoor decentraliseren van (het beheer van) data mogelijk blijft. In dat kader zal ZORG-AB aansluiten op de ontwikkelingen van de Architectuurboard en TSV, waarbij leveranciers hun technische adresinformatie onder eigen beheer willen houden. Het is de vrije keuze van de leveranciers waar ze de gegevens willen beheren. Voorwaarde is uiteraard dat het daar veilig en goed beschikbaar is.*

Feitelijk wordt hier gesteld: ZORG-AB is federatief opgezet (en voldoet daarmee aan het manifest van de DIZRA) omdat het technisch gezien **niet onmogelijk** wordt gemaakt dat er meerdere adresboeken bestaan. Wij hebben de indruk dat de DIZRA daarmee onjuist wordt geïnterpreteerd. Laten we de tekst uit het DIZRA manifest erbij pakken:

> *8. In het informatiestelsel wordt **federatief** samengewerkt aan afspraken voor data en voor diensten. Iedereen implementeert deze afspraken en is aanspreekbaar op het nakomen van de afspraken en de kwaliteit van de implementatie.*

En in de definities:

> ***Federatie***
> *Een afsprakenstelsel maakt afspraken over een federatief stelsel van diensten. De term federatie wordt gebruikt om aan te geven dat **iedere deelnemer** in het netwerk **autonoom** is en zelf verantwoordelijk is voor de implementatie en het operationeel houden van **diensten**.*

Ook lezen we onder Netwerkactor:

> *DIZRA gaat uit van datagestuurd werken. Dit betekent dat we data modelleren en publiceren. Een bronhouder van data is de uitgever van de data. We gaan uit van data die **beschikbaar is bij de bron** en waarvan bekend is dat publicatie waardevol is. Deze data willen we FAIR maken.*

Iedere deelnemer in het netwerk is dus autonoom en implementeert zelf de gemaakte afspraken. Iedere deelnemer is zelf in beheer van de eigen data. De deelnemers in dit voorgestelde netwerk zijn dus **niet beperkt** tot de beheerders van geaggregeerde adresboeken. Deelnemers zijn juist ook de partijen die **opgenomen staan** in het adresboek en partijen die andere **registers beheren** (zoals het CIBG en Vektis), eventueel vertegenwoordigd door hun softwareleveranciers.

Wij kunnen daarom niet anders concluderen dan dat ZORG-AB **niet voldoet** aan de DIZRA, en ook **niet voldoet** aan punt vier van het Nuts manifest.

Wie is leidend?

In de bij het voorstel geleverde implementatiehandleiding wordt een adresboek beschreven dat gegevens gaat importeren uit de volgende bronnen (hoofdstuk 1):

- *Vektis AGB Services*
- *Het clientèlebestand (BI-bestand) van VZVZ*
- *UZI LDAP*
- *Een live koppeling met het applicatieregister van het LSP*
- *Mogelijkheden om MedMij Gegevensdiensten op te slaan en te zoeken op MedMij-naam*

Daarbij krijgt één van deze bronnen de rol van *author*. Dat wil zeggen dat die bron leidend is, en dat alleen die bron mutaties kan aanbrengen in het betreffende model. Wij vragen ons af wat er gebeurt wanneer verschillende bronnen gegevens over **dezelfde** organisatie of zorgverlener hebben (wat toch aannemelijk lijkt), en in het bijzonder wat er gebeurt als die gegevens niet **overeenkomen**? Welke bron is dan leidend, wie heeft er dan “gelijk”, en hoe gaat VZVZ als beheerder van ZORG-AB dit gelijk vaststellen?

Daarnaast wordt er in het voorstel het volgende geponeerd:

> ***Zijn er alternatieven voor de bouwsteen?***
> *Op dit moment is er nog geen alternatief beschikbaar.*

Dit lijkt ons niet geheel juist. Er is **nog een adresboek** dat gegevens over alle zorginstellingen van Nederland bijhoudt, en dit doet op basis van een wettelijke taak: het LRZa. We kunnen op de voorpagina van hun website lezen dat zij een soortgelijke importering doen, van een deels overlappende dataset:

> ***Gegevens uit 5 bronnen***
> *Het LRZa biedt een uitgebreid overzicht van het zorglandschap. Hiervoor koppelt het LRZa informatie aan elkaar uit het Handelsregister van de Kamer van Koophandel, het AGB-register (Algemeen Gegevens Beheer Zorgverleners) van Vektis en het BIG-register. Daarnaast ontsluit het LRZa ook informatie uit het openbaar databestand kwaliteitgegevens zorg van Zorginstituut Nederland en de Jaarverantwoording Zorg.*

Zoals gezegd zijn wij in alle gevallen geen voorstander van één centraal adresboek van zorgverleners. Maar is het, geredeneerd vanuit centraal beleggen, niet veel voor de hand liggender om de MedMij gegevensdiensten, LSP applicaties en andere technische *endpoints* toe te voegen aan het LRZa? Dit is immers **een reeds belegde overheidstaak**. Het is ons inziens **onwenselijk en onnodig** om deze taak te dupliceren en bij een private vereniging te beleggen.

De doelstelling van het LRZa zou zeker goed op MedMij aansluiten:

> *Het doel van het Landelijk Register Zorgaanbieders (LRZa) is om duidelijk te maken wie, waar, welke zorg verleent en met welke bevoegdheid.* ***Zo heeft de burger inzicht in waar hij welke zorg kan verkrijgen.***

Privacy & Security

In de computerbeveiliging kennen we het fenomeen van de ***man in the middle***. Wanneer Alice een bericht wil sturen naar Bob (een e-mail, een telefoontje of een compleet patiëntendossier) moet Alice zich ervan vergewissen dat zij echt met Bob spreekt. Want het is niet ondenkbaar en soms lastig te detecteren dat een *man in the middle* (hier genaamd Mallory) alle berichten onderschept en doorstuurt naar Bob, en vice versa.

Mallory is dan in staat om **alle communicatie** tussen Alice en Bob af te luisteren en zelfs te manipuleren. Zo'n situatie kan bijvoorbeeld ontstaan wanneer Mallory in staat is om Alice een **foutief adres** van Bob te verstrekken; een adres dat in feite van Mallory is. In onze zorg-context kan zo'n situatie bijvoorbeeld tot een datalek van patiëntgegevens leiden, of kan het zelfs dodelijke gevolgen hebben wanneer een bericht wordt gemanipuleerd en de verkeerde medicatie wordt voorgeschreven.

Voor wie zich nog de handgeschakelde telefooncentrale kan herinneren: Mallory is de telefoniste op de centrale die jouw gesprek mee kan luisteren of jouw verbinding kan beïnvloeden.

Het grootste probleem op het vlak van privacy en security van ZORG-AB is dat het zich opwerpt als de "telefooncentrale" van de Nederlandse zorg. VZVZ zegt met dit voorstel: wij verzamelen, beheren en faciliteren alle benodigde contactgegevens, zodat jullie je daar geen zorgen over hoeven te maken. En als je met iemand wilt communiceren, dan bevraag je ZORG-AB, en ZORG-AB vertelt je via welke kanalen je die andere partij kunt bereiken.

Maar ZORG-AB geeft daarbij **geen harde waarborgen** dat de gegevens die zij heeft juist zijn, anders dan het vertrouwen dat wij allen moeten stellen in de processen van de beheersorganisatie. De gehele

Nederlandse zorg zal er dus op moeten vertrouwen dat deze telefooncentrale naar behoren werkt, en er bijvoorbeeld geen fouten worden gemaakt in het aan elkaar koppelen van verschillende datasets. Of dat er medewerkers een extra zakcentje gaan verdienen zoals laatst bij de GGD het geval bleek. Hiermee wordt ZORG-AB een zogenaamde **security-hotspot**: een aantrekkelijk doelwit voor hackers.

Eén van de manieren om dit *man in the middle* probleem op te lossen is door Bob zijn contactgegevens cryptografisch te laten ondertekenen. Alice kan dan controleren of de ondertekening van de gegevens van Bob inderdaad klopt, en zo ja dan weet zij zeker dat ze de juiste gegevens heeft ontvangen. Het maakt dan niet meer uit wie de contactgegevens beheert of verstrekt, omdat Alice die waarborgen autonoom kan controleren. Daarna kan er een versleutelde verbinding tussen Alice en Bob worden opgezet, en heeft Mallory het nakijken. Dit soort mechanismen maken dat we **al jaren** met vertrouwen onze bankzaken online kunnen doen, zelfs op openbare WiFi netwerken.

De punten zeven en acht uit het Nuts manifest laten zien dat wij van mening zijn dat het beter kan en beter moet:

> **7. Security by design**
> *Wij geloven dat elk systeem dat wil kunnen schalen er al in de ontwerpfase vanuit moet gaan dat er partijen in het netwerk kunnen deelnemen die **niet te vertrouwen** zijn, en dat ook kwaadwillenden steeds slimmer worden. We willen te allen tijde **voorkomen** dat onze infrastructuur een onbevoegde in staat stelt om medische informatie over mensen te bekijken, te veranderen of te verwijderen.*
>
> **8. Cryptografische basis**
> *Wij geloven dat de technologie en de tijd rijp zijn voor een systeem gebaseerd op **cryptografische principes**. We willen garanties kunnen geven over identiteiten en **toegang tot data** die verder gaan dan "het is zo geconfigureerd". Wij geloven dat we alleen met zo'n oplossing het **vertrouwen** van de hele markt—en uiteindelijk van de burger—kunnen winnen.*

Onze beveiligingsexperts zijn van mening dat de bij ZORG-AB voorgestelde organisationele benadering van vertrouwen **niet meer bij de stand van de techniek past**. Wij vinden het ook opmerkelijk dat er in het voorstel weinig gesproken wordt over dit soort beveiligingsrisico's, terwijl een adresboek toch (zoals beschreven) de eerste cruciale stap is in veilige communicatie. Wat in deze stap verkeerd gaat heeft verstrekkende gevolgen voor de integriteit en vertrouwelijkheid van de rest van de communicatie.

We moeten het nu stellen met de volgende zeer summiere passage in §3.6.b:

> *Beveiliging: ZORG-AB voldoet aan wet- en regelgeving AVG, Wabvpz, NEN7512. Toegang wordt verkregen via een PKIO-servercertificaat of UZI-servercertificaat.*

En deze passage in §3.6.g:

> ***Beschrijf mogelijke beveiligings- of privacy risico's:***
> *Alle risico's zijn voldoende afgedekt met mitigerende maatregelen. Toegang tot ZORG-AB via Zorgnet (opvragen en muteren) of via Internet (alleen opvragen) door middel van respectievelijk UZI-servercertificaat en PKIO-certificaat in combinatie met whitelisting van de IP-adressen. Pentest is reeds met succes uitgevoerd. De beveiligings- en privacy risico's bestaan hieruit:*
> *− Ten onrechte vermeld in ZORG-AB, dan is of een onderliggend register in de fout gegaan of*

(onder verantwoordelijkheid van de zorgaanbieder) een persoon toegevoegd die geen toestemming heeft gegeven voor publicatie.
− Wijzigrechten van een zorgaanbieder in ZORG-AB worden verkregen via een PKIO-servercertificaat of UZI-servercertificaat. Het betreft hier alleen rechten voor het muteren. Wijzigen is alleen toegestaan als de zorgaanbieder gebruik maakt van een GZN (Zorgserviceprovider, Goedbeheerd Zorg Netwerk).
− Raadplegen is alleen toegestaan mits de organisatie (middels een PKIO-servercertificaat) is toegevoegd aan de whitelist van ZORG-AB.
− Alleen het gebruik wordt gemonitord, niet de inhoudelijk uitwisseling. Er is immers geen inhoudelijke uitwisseling.
− Het ZORG-AB Integratie Proces (ZIP) bewaakt de integriteit en de kans op langdurige foutieve informatie in ZORG-AB.

Dit is alles wat er in het voorstel wordt beschreven over privacy en security.

Dit vertelt ons hoe de API van ZORG-AB beveiligd is. Maar het vertelt ons niets over welke maatregelen er getroffen worden om de integriteit van de contactgegevens te garanderen, anders dan dat er blijkbaar een proces bestaat (niet meegeleverd) om **langdurige** fouten te voorkomen. Hoe zit het dan met kortdurende fouten? Hoe wordt de data opgeslagen? Welke (helpdesk-)medewerkers hebben mutatie-rechten bij VZVZ? En welke bij uitvoerder DXC? En onder welke voorwaarden? Hoe wordt dat technisch afgedwongen? Hoe worden fouten *up-stream* bij de aanleverende bronnen uitgesloten?

En de allerbelangrijkste vraag: waarom staan contactgegevens niet **cryptografisch ondertekend** (bijvoorbeeld met het UZI certificaat van de zorginstelling) in ZORG-AB, zodat iedereen zich van de juistheid ervan kan vergewissen?

Het feit dat hier geen enkele aandacht aan besteed wordt baart ons zorgen. Het doet ons erover twijfelen of de indieners zich realiseren hoe **gevoelig** de voorziening is. En het doet ook de vraag rijzen hoe de kennis van de indieners zich ontwikkelt in relatie tot eerdere kritische consultaties, feedback van de architectuurboard van het informatieberaad, en de ontwikkelde stand van de techniek.

Openheid & Uitbreidbaarheid

Tenslotte een aantal losse punten van zorg over de openheid en toekomstige uitbreidbaarheid van de voorgestelde voorziening.

Het datamodel dat is gepresenteerd in de implementatiehandleiding spreekt van drie soorten “Electronic Services”:

1. IHE ElectronicService
2. LSP Application
3. MedMij Gegevensdienst

Graag horen wij van de indieners of dit beschouwd wordt als een **uitputtende lijst**, of dat er al andere typen “Electronic Services” op stapel staan. Wij kunnen ons namelijk niet voorstellen dat met deze drie

categorieën alle voor de VIPP regelingen en voor de prioritaire zorgprocessen benodigde uitwisselingen zijn afgedekt.

Om gegevens in ZORG-AB te kunnen muteren moeten zorginstellingen gebruik maken van het Zorgnet. Dit wordt gepresenteerd als een beveiligingsmaatregel. Wij kunnen ons echter niet voorstellen dat een **privaat netwerk**, met bijbehorende hoge abonnementskosten, nog noodzakelijk is voor de beveiliging van systemen die zelf in toenemende mate rechtstreeks met het Internet verbonden zijn. We zijn van mening dat dit de adoptie zal remmen, en dat hier blijkbaar gekozen wordt voor *security through obscurity* in plaats van echte beveiliging, zoals ook hierboven in het hoofdstuk *Privacy & Security* besproken.

In het voorstel wordt gesproken over een proces van wijzigingen aan ZORG-AB, op aanvraag van veldpartijen danwel leveranciers, in §3.5.b:

> ***Op welke wijze zijn deze partijen betrokken bij de besluitvorming met betrekking tot deze bouwsteen?***
> *ZORG-AB wordt op vraag van en samen met de veldpartijen doorontwikkeld. Dit is een transparant proces (inclusief publicatie op website, nieuwsbrieven, workshops.).*

En in §3.1.d:

> *ICT-dienstverleners, leveranciers kunnen wijzigingsverzoeken indienen voor uitbreiding van de functionaliteit van ZORG-AB.*

Het is ons echter **niet duidelijk** hoe deze processen eruit zien, wat de doorlooptijd zal zijn en op welke wijze partijen invloed kunnen uitoefenen op de doorontwikkeling van het systeem.

Tenslotte willen wij de indieners verzoeken om alle gepresenteerde onderdelen van ZORG-AB, evenals de gebruikte configuraties **publiek te maken**. Bijvoorbeeld in de vorm van Open Source software. Alleen dan kan door beveiligingsexperts uit het hele land worden vastgesteld of de beveiliging van ZORG-AB ook daadwerkelijk correct is geïmplementeerd, en eraan bijdragen dat die waar nodig nog wordt verbeterd. Daarnaast zou de publicatie van een onafhankelijke security audit met enige regelmaat moeten uitwijzen of die gepubliceerde code en configuraties ook daadwerkelijk overeenkomen met de versies die in praktijk gebruikt worden.

Net als in onze reactie op de open consultatie van Mitz roepen we ook in deze reactie de auteurs van dit voorstel op om hier nader met ons over na te denken en om de opgedane kennis en documenten open (*public domain*) beschikbaar te stellen.

En we sluiten wederom af met de oproep: Laten we ophouden te redeneren vanuit een specifiek product van een specifieke leverancier. Dat levert altijd centralistische oplossingen op die meer vragen dan antwoorden opleveren op zaken als vertrouwen, macht en soevereiniteit. We hebben nu de kans om met een schone lei te beginnen, met de stand van de techniek van vandaag in plaats van die van rond de millenniumwisseling. Laten we een federatief stelsel ontwerpen, vanuit **samenwerking in de gehele markt** en het maken van open afspraken waar iedereen vrijelijk bij kan aansluiten.

Vragen aan de indieners

1. Wat is eigenlijk, in de ogen van de indieners, allemaal adresinformatie? Waar eindigt de scope van ZORG-AB?
2. Waarom is er niet gekozen voor een nauwere scope, zoals *service discovery*?
3. Zijn de indieners het met stichting Nuts eens dat er geen enkele reden is om aan te nemen dat centrale regie automatisch tot een betere integriteit en vertrouwelijkheid leidt?
4. Waarom wordt er beweerd dat het voorstel aan de DIZRA voldoet, wanneer dit duidelijk niet het geval is? Welke stappen gaan de indieners zetten om hier alsnog aan te voldoen?
5. Wat gebeurt er wanneer verschillende geïmporteerde bronnen gegevens over dezelfde organisatie of zorgverlener bevatten? En wat als die gegevens niet overeenkomen? Welke bron is dan leidend, wie heeft er dan “gelijk”, en hoe gaat VZVZ als beheerder van ZORG-AB dit gelijk vaststellen? Hoe worden fouten *up-stream* bij de aanleverende bronnen uitgesloten?
6. Waarom wordt er voorbijgegaan aan het LRZa als mogelijke houder van een zorgadresboek? Waarom zouden we deze belangrijke taak bij een private vereniging beleggen, wanneer die taak feitelijk al publiek belegd is?
7. Hoe wordt de adresdata opgeslagen? Welke (helpdesk-)medewerkers hebben mutatie-rechten bij VZVZ? En welke bij uitvoerder DXC? En onder welke voorwaarden? Hoe wordt dat technisch afgedwongen?
8. Waarom staan contactgegevens niet met harde waarborgen—zoals een cryptografische handtekening van de zorginstelling—in ZORG-AB, zodat iedereen zich van de juistheid ervan kan vergewissen?
9. Worden de drie genoemde typen “Electronic Services” beschouwd als een uitputtende lijst, of staan er op korte termijn meer typen op stapel?
10. Hoe kan het dat een aansluiting op Zorgnet verplicht gesteld wordt om mutaties van de eigen gegevens digitaal door te voeren?
11. Hoe ziet het wijzigingsproces van ZORG-AB eruit? Wat is daarvan de doorlooptijd en op welke wijze kunnen partijen invloed uitoefenen op de doorontwikkeling van het systeem?
12. Zal ZORG-AB publiek gemaakt worden in de vorm van Open Source software, zodat beveiligingsexperts zich van de goede werking ervan kunnen vergewissen? Komt er een bijbehorende periodieke security audit, om aan te tonen dat wat gepubliceerd is gelijk staat aan wat er in productie staat?