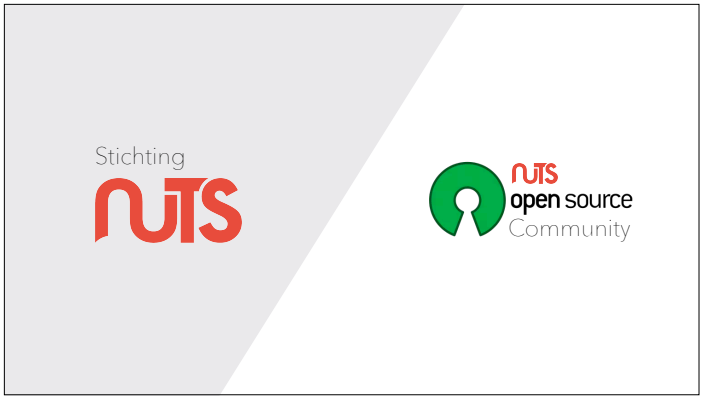
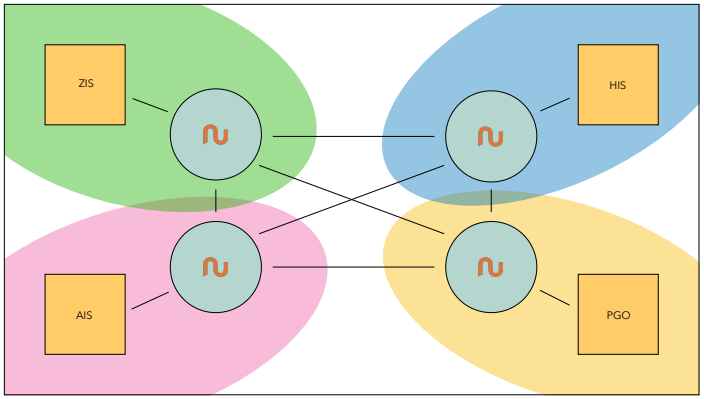
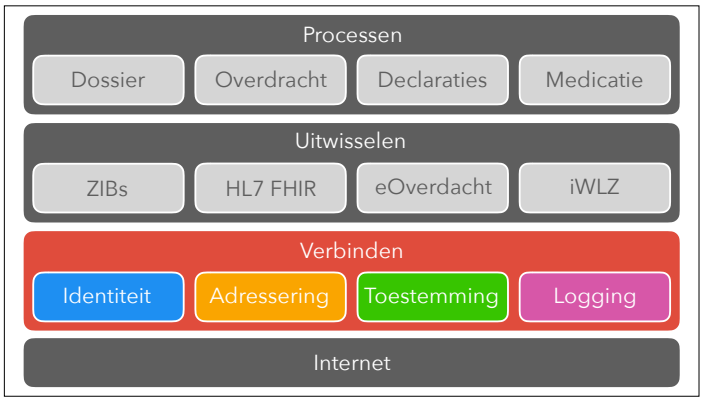


Ongeveer een jaar geleden zijn we een initiatief gestart dat we Nuts noemen. Dat doen we in twee vormen: we hebben in oktober vorig jaar de onafhankelijke stichting Nuts opgericht, die als doelstelling heeft meegekregen om samenwerking te bevorderen tussen softwareleveranciers en onderzoek en ontwikkeling van software te stimuleren. Dat stimuleren doen we door middel van onze Open Source community waarin leveranciers met elkaar componenten ontwikkelen en beschikbaar stellen die we allemaal nodig hebben en waarop we niet met elkaar hoeven te concurreren.

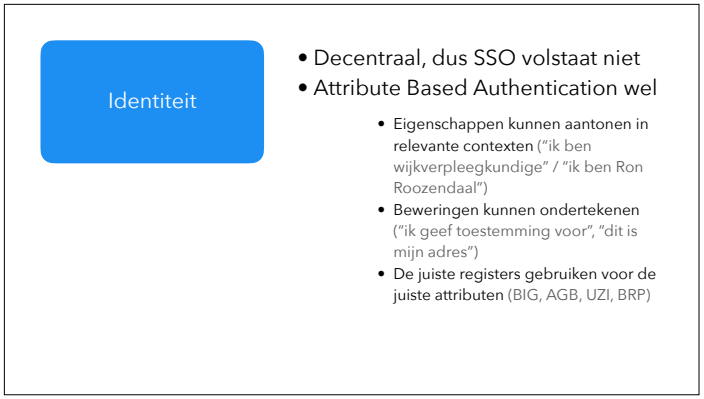
Onze eerste stap was het formuleren van een manifest van acht punten op basis waarvan de deelnemende partijen met elkaar willen samenwerken. De volledige uitwerking van dit manifest kun je vinden op https://nuts.nl/manifest



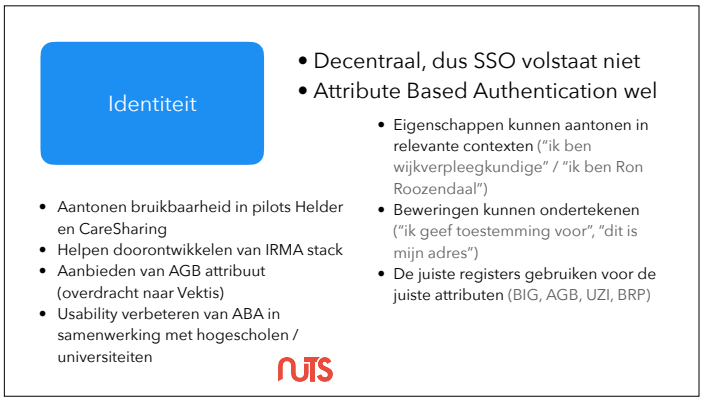
De oplossing die Nuts beoogt is eigenlijk een heel simpele. Elke softwareleverancier beheert zelfstandig een stuk Open Source software, dat we een “Nuts-node” noemen. Elke “Nuts-node” legt verbindingen met andere nodes wanneer achterliggende softwarepakketten gegevens met elkaar uitwisselen.
Het beheer van een node representeert hierdoor een proportioneel deel van de infrastructurele kosten, dat mee-schaalt met het gebruik van de applicatie van de leverancier. En omdat gegevens rechtstreeks van het (juridische) domein van de ene zorgverlener naar het (juridische) domein van de andere zorgverlener worden verzonden hoeven er geen additionele bewerkersovereenkomsten getekend te worden.



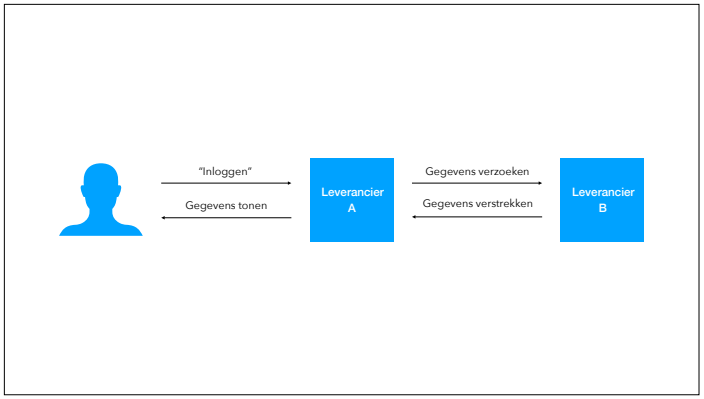
In die nieuwe decentrale wereld hebben we vier thema’s geïdentificeerd die een uitdaging gaan vormen. Het betreft het decentraal identificeren van personen (authenticatie), het decentraal beheren van toestemmingen (autorisatie), het decentraal adresseren van systemen (adresboek) en het decentraal loggen van wat er heeft plaatsgevonden. Dat zijn ook precies de vier thema’s waar we ons nu op focussen, zodat we systemen met elkaar kunnen verbinden. Daarmee is wat Nuts doet proces- en uitwisselingsstandaard-agnostisch. Anders gezegd: Nuts “bemoeit” zich alleen met het rode vlak.
Er is ons gevraagd om op elk van deze blokjes een stukje dieper in te zoomen, dus dat zullen we in de rest van deze presentatie doen.



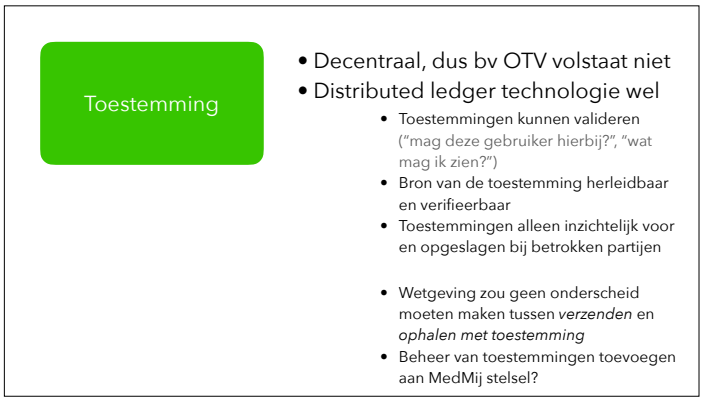
Wat betreft identiteit: Omdat wij actief op zoek zijn naar een decentrale oplossing voldoet bijvoorbeeld een single sign on methode niet. Die is inherent centraal georganiseerd. Een attribute based authentication methode voldoet wel, mits we daarmee kunnen bewijzen dat we bepaalde eigenschappen hebben en zaken kunnen ondertekenen. Wij zijn ook niet van plan om een "Nuts login" te introduceren of een eigen identiteitsregister aan te leggen als we het even kunnen voorkomen. Liever gebruiken we bestaande registers zoals de BRP voor het BSN of het BIG register voor de kwalificaties van artsen.



Nuts werkt aan dit onderwerp door aan te tonen dat een ABA methode gebruikt kan worden in de zorg middels de Helder en CareSharing use-cases. Onze community helpt actief aan de ontwikkeling van de IRMA stack en de usability van ABA. IRMA is momenteel de enige attribute based authentication implementatie die in Nederland actief is. En we bieden een attribuut aan op basis van het Vektis AGB register, dat we in overleg met Vektis aan hen zullen overdragen.



Het aantonen van identiteit willen we op zo'n manier doen dat gebruikers in een netwerk kunnen bewijzen wie ze zijn. Daarvoor gebruiken we "attribute based authentication" in combinatie met het ondertekenen (signen) van een "contract". Daardoor kunnen we gebruikers van één systeem zich identificeren bij een achterliggend tweede systeem waar ze niet als gebruiker bekend zijn, zonder SSO oplossing.



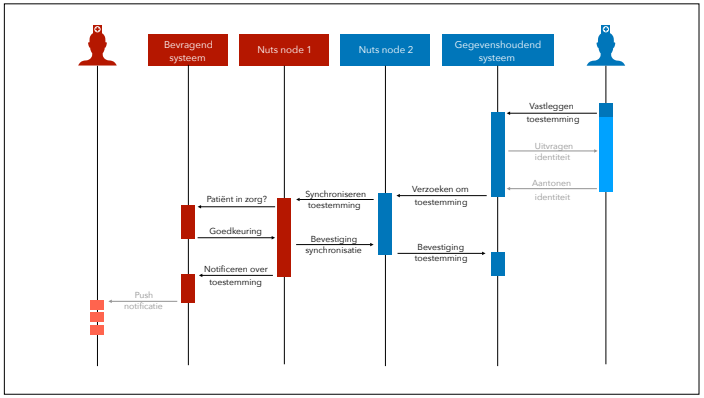
Op het gebied van toestemming zoeken we wederom een decentrale oplossing, waardoor initiatieven zoals een online toestemmingsvoorziening (uitvloeisel van GTS) niet volstaan als je ze naast ons manifest legt. We zijn daarom nu een oplossing aan het bouwen op basis van distributed ledger technologie. We willen een toestemmingsregister bouwen waartegen we (performant) binnenkomende verzoeken om informatie kunnen valideren, en waarbij toestemmingen alleen opgeslagen worden bij de betrokken partijen.
Er is discussie over het afschaffen van het wettelijk onderscheid tussen het verzenden en het ophalen van informatie. Wij zouden aan die discussie willen toevoegen dat het ophalen van informatie **met toestemming** gelijkwaardig zou moeten zijn aan het verzenden van informatie. Uiteindelijk is er in technische zin altijd een expliciete toestemming nodig, omdat we anders de toegang niet kunnen bewaken.
We zien een toekomst voor ons waarin burgers ook inzage krijgen in, of misschien

Toestemming

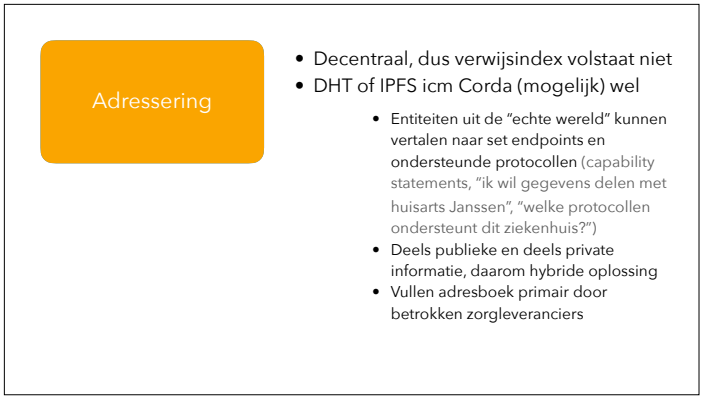
- Ontwikkeling van decentraal toestemmingsregister is gestart (obv R3 Corda)
- Eerste demo's zijn functioneel, nu naar productie
- Ontwikkelen tools om binnenkomende verzoeken makkelijk te valideren tegen register

- Decentraal, dus bv OTV volstaat niet
- Distributed ledger technologie wel
  - Toestemmingen kunnen valideren ("mag deze gebruiker hierbij?", "wat mag ik zien?")
  - Bron van de toestemming herleidbaar en verifieerbaar
  - Toestemmingen alleen inzichtelijk voor en opgeslagen bij betrokken partijen
- Wetgeving zou geen onderscheid moeten maken tussen *verzenden* en *ophalen met toestemming*
- Beheer van toestemmingen toevoegen aan MedMij stelsel?

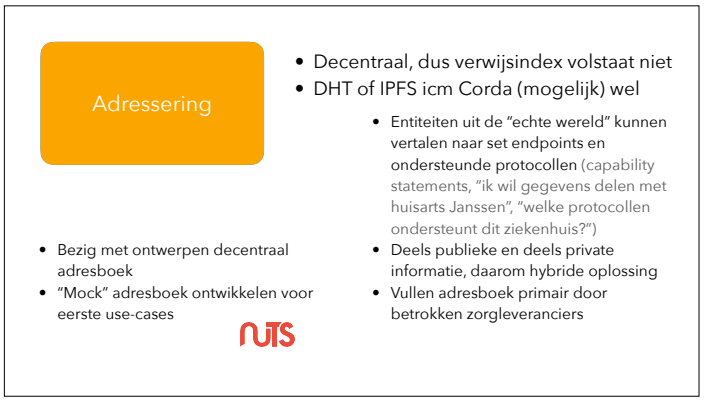
Nuts is op dit thema bezig met de ontwikkeling van een toestemmingsregister op basis van de decentrale ledger-technologie Corda. We hopen daarmee komende zomer in productie te kunnen gaan voor de eerste pilots met echte dossiers.



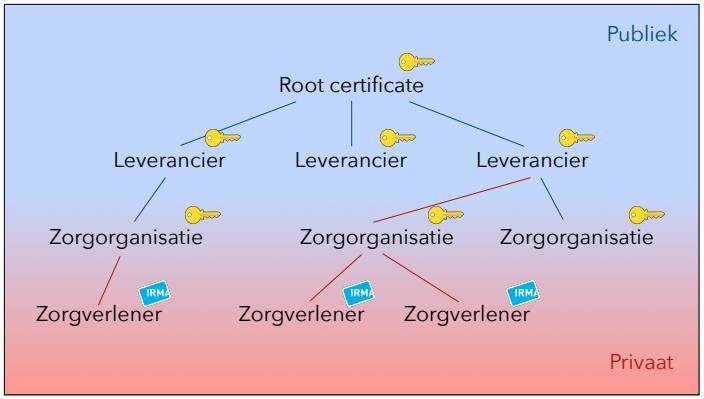
In deze sequence diagram laten we zien hoe een gebruiker van een gegevenshoudend systeem in "de Nuts wereld" een toestemming vastlegt namens een patiënt voor een gebruiker in een ander systeem.



Op het vlak van adressering zoeken we ook een decentrale oplossing, dus zaken zoals centrale verwijsindices vallen af. We kunnen waarschijnlijk wel iets moois bouwen op basis van Distributed Hash Tables of Interplanetary Filesystem in combinatie met zoiets als Corda voor een hybride oplossing. We willen met een adresboek entiteiten uit de "echte wereld" kunnen opzoeken in ICT systemen en die vervolgens vertalen naar capacity statements over wat het systeem van die andere zorgleverancier ondersteunt.



Nuts is bezig dit systeem te ontwerpen en de nodige APIs daarvoor te definiëren. Daarnaast ontwikkelen we voor de eerste use-cases een "mock" adresboek dat zich vanuit het perspectief van ECD systemen wel gedraagt zoals we dat willen, maar eigenlijk nog niet zo decentraal is als we willen. Op die manier kunnen we het "mock" component op enig moment makkelijker vervangen door de "echte" versie.



Een decentraal adresboek kent twee grote uitdagingen. Ten eerst: het is deels privaat en deels publiek. Relaties tussen ICT leveranciers en een root certificate zijn (noodzakelijk) publiek, relaties tussen zorgorganisaties en leveranciers meestal ook, maar de relaties tussen zorgorganisaties en natuurlijke personen zijn dat niet. Daarom hebben we een hybride oplossing nodig waarbij een deel van het adresboek voor iedereen toegankelijk is en een deel van het adresboek “on a need-to-know basis”. De tweede uitdaging is de betrouwbaarheid van de informatie in het adresboek. Onze insteek is dat elke partij zijn eigen gegevens beheert. Door middel van cryptografische ondertekeningen kunnen we de echtheid van die gegevens valideren. Voor organisaties gebruiken we daar private keys voor en voor individuen gebruiken we attribute based authentication.

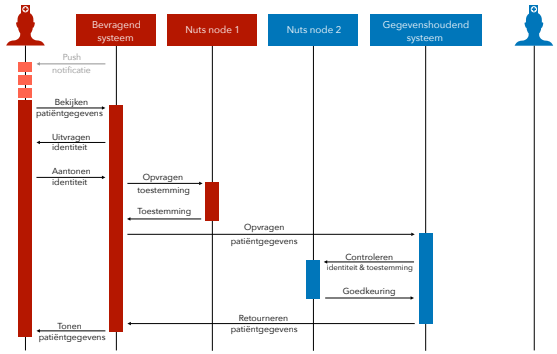
Op het vlak van logging zijn we eigenlijk een stapje verder dan voor de andere thema’s, want logging gebeurt al decentraal. Alleen kunnen we de logs momenteel nog niet op een uniforme manier uitwisselen. Het zou veel mooier zijn als een patiënt in zijn PGO kan zien wie er welke gegevens heeft gedeeld of ingezien, en waarom. Ook dat zou een mooie toevoeging kunnen zijn aan het MedMij stelsel. Ook voor logging geldt dat gegevens “on a need-to-know basis” gedeeld moeten worden omdat de logs privacy-gevoelige informatie bevatten.

Logging

- Decentraal, zoals het al is
- Corda of soortgelijk kan volstaan
  - Append-only logging faciliteit voor "gedeelde waarheid" ("wie heeft mijn gegevens ingezien?", onderzoek naar een medewerker of fraude)
  - Toegang tot logging slim autoriseren
  - Logging alleen inzichtelijk voor en opgeslagen bij betrokken partijen
  - Inzicht in logging toevoegen aan MedMij stelsel?

- Logging decentraal bij elke partij vastleggen
- Nadenken over standaard formaat en APIs waarmee logs opgehaald kunnen worden
- Nadenken over de "volgende generatie" op basis van DLT zoals Corda
- Samenwerking met Common Ground?

Binnen de Nuts community leggen we logs momenteel ook bij elke partij apart vast. We denken na over standaardisatie van formats en APIs om die logs met elkaar uit te kunnen gaan wisselen, en over de toekomstige mogelijkheden om logs ook gedistribueerd in een netwerk vast te gaan leggen. We houden het Common Ground initiatief hierbij goed in de gaten.



In deze sequence diagram laten we zien hoe een gebruiker van een bevragend systeem die toestemming heeft gekregen gegevens ophaalt bij een gegevenshoudend systeem. Merk op dat de communicatie van de daadwerkelijke patiëntgegevens niet via de Nuts nodes hoeft te lopen, en dus in elke standaard en via elk protocol kan plaatsvinden, bijvoorbeeld door het uitwisselen van ZIBs op basis van FHIR.

Wat hebben we nodig?

- De politieke ruimte om te **experimenteren**
  - Uitgifte betrouwbare attributen
  - Wetgeving & juridische sparring
- PKI infrastructuur en beheer van **root keys**
  - Attributenstructuur
  - Certificatenstructuur
- Goede **open standaarden** en certificering voor de "gegevenslaag"

Als leverancierscommunity hebben we behoefte aan de ruimte om te kunnen experimenteren. De overheid zou hierin kunnen stimuleren door betrouwbare attributen uit te geven (BRP, BIG, etc) op basis waarvan de sector verder kan. Daarnaast zijn wij op zoek naar een sparring partner voor wetgeving en juridische zaken. Een aantal punten waar wetgeving zou kunnen helpen zijn al benoemd, zoals het onderscheid tussen data verzenden of ophalen met toestemming.
Daarnaast hebben we een PKI infrastructuur nodig en het beheer van keys. Momenteel ligt die verantwoordelijkheid voor attributen bij de stichting Privacy by Design en voor de certificaten bij de Nuts stichting. Maar wij zijn niet op zoek naar die verantwoordelijkheid of die macht, dus het zou fijn zijn als dit op een bepaald moment overgenomen kan worden door een ander betrouwbaar orgaan, zoals de overheid.
Tenslotte: als we al deze zaken geregeld hebben dan kunnen we nog steeds **helemaal niets**. We hebben dan alleen nog maar een hele reeks aan voorwaardelijke zaken geregeld. Vervolgens hebben we goede open standaarden nodig om daadwerkelijk informatie uit te wisselen, zaken als eenheid van taal in dossiervoering en ZIBS. Daar wordt al aan gewerkt, en dat is ook van groot belang voor Nuts.

Take-away message

- Het **kan** decentraal
- Het kan **beter/veiliger/minder marktverstorend** decentraal
- En **weest welkom!**

We willen jullie graag achterlaten met deze boodschap: het **kan** decentraal. En als we het decentraal oplossen kunnen we gegevens beter en veiliger en meer privacy bewust uitwisselen, met minder marktverstoring door de overheid.

En weest welkom om mee te komen doen. Hoe meer leveranciers daadwerkelijk capaciteit beschikbaar stellen om mee te helpen ontwikkelen, hoe sneller we kunnen gaan.