NUTS toont genadeloos manco's in Mitz als beoogde online toestemmingsvoorziening

Op 21 en 22 september 2020 schreef ik op deze website over het plan van Zorgverzekeraars Nederland(ZN) en VZVZ om via het Informatieberaad Zorg een centrale online toestemmingsvoorziening te realiseren. Het gaat om een centraal computersysteem genaamd Mitz voor het vastleggen van toestemmingen om elektronische uitwisseling van zorgdata te faciliteren. Daartoe organiseerde het Informatieberaad een "open consultatie" waarbij men ideeën en adviezen kan inbrengen. Naar nu bekend is heeft de Stichting NUTS, net als ik, ook een inbreng geleverd. Die inbreng is bijzonder kritisch over Mitz. In hun reactie in het kader van de consultatie laat men genadeloos zien hoe Mitz als online toestemmingsvoorziening geen echte oplossing biedt. Mitz zou leiden tot een central point of failure, een monopolie-positie en ook een ongewenste afhankelijkheid van één leverancier. Met als gevolg een vendor lock-in. NUTS staat daarentegen een decentrale oplossing voor: een gedistribueerd model van communicatie, vergelijkbaar met het internet.

NUTS

Het is een initiatief van softwareleveranciers in de zorg die pre-concurrentieel samenwerken aan open standaarden waarmee ze de zorg vooruit willen helpen. Zie hiervoor het manifest van NUTS. De inbreng voor de open consultatie, waarvan ik in de eerste alinea de link publiceerde, staat op hun webpagina 'Over de stichting' onder de rubriek Documenten. In deze inbreng staat op pagina 2 en 3 onder het hoofdstuk Vrije markwerking en innovatie fundamentele kritiek over Mitz. Niet

alleen zou een toestemmingsvoorziening als Mitz, als die er zou komen, de toegang tot alle gezondheidsdata van Nederland beheren. Daarmee zou Mitz volgens NUTS ook de instantie worden die indirect die data beheert. NUTS bekritiseert ook de gedachte die VZVZ op pagina 15 in hoofdstuk 4.3.5 van haar Mitz-ontwerp heeft over het plan dat naast een landelijke toestemmingsvoorziening ook regionale kunnen bestaan. Daardoor ontstaat er voor de patiënt een lappendeken van verschillende (deel)oplossingen.

Kritiek op cryptografische basis

Op pagina 4 van de reactie van NUTS gaat men uitgebreid in op de cryptografische waarborgen die de Vereniging van Zorgaanbieders Voor Zorgcommunicatie, verantwoordelijke voor het Landelijk SchakelPunt, zegt te geven bij Mitz. VZVZ schrijft over drie tokens die deze waarborgen zouden moeten geven: (1) het mandaattoken, (2) het inschrijftoken plus 3. het transactietoken, dat nodig is voor het koppelvlak met Mitz. De eerste twee zijn ondertekend door de UZI-pas. NUTS constateert dat geen van de drie tokens daadwerkelijk de afgegeven toestemming ondertekent met een authenticatiemiddel. Het zijn alle drie tokens om de toestemmingsvoorziening vertrouwen te geven in de afgifte van de toestemming, niet de dossierhouder.

Onweerlegbaarheid

NUTS geeft als alternatief:

“Om de dossierhouders in staat te stellen om de onweerlegbaarheid van toestemmingen onafhankelijk te kunnen valideren moeten deze toestemmingen zelf cryptografisch worden ondertekend met een sterk authenticatiemiddel. Daarmee kunnen de stappen 1 en 2 uit de bovenstaande opsomming over worden geslagen en wordt er alleen vertrouwen gelegd in de gebruikte authenticatiemiddelen. Dit hebben we ook beschreven in de toelichting bij punt acht van ons manifest: Identiteit is iets

dat je persoonlijk inbrengt, een unieke sleutel op basis waaraan je te herkennen bent, toestemmingen kunt ondertekenen, en jouw eigen gegevens kunt ontsleutelen. Dankzij die unieke sleutel kunnen we onomstotelijk aantonen door wie toestemmingen zijn afgegeven en wie het verzoek doet om data op te halen uit een ander systeem."

Privacy- en security-hotspot

De professionals bij NUTS maken zich grote zorgen over dat Mitz een privacy en veiligheidsrisico gaat vormen. Zij stellen dat in de toestemmingsvoorziening relaties opgeslagen komen te liggen tussen natuurlijke personen en (groepen van) zorgaanbieders. Daarnaast worden ten behoeven van inzage voor de patiënt, relaties vastgelegd tussen zorgaanbieders die communiceren over een persoon. VZVZ beschrijft dat in hun stuk in hoofdstuk 4.1.1. Uit die relaties kunnen gemakkelijk ziektebeelden afgeleid worden. Dan worden er dus effectief bijzondere persoonsgegevens van (potentieel) alle Nederlanders in Mitz opgeslagen. Dat maakt de voorziening tot een privacy-hotspot. NUTS stelt daarnaast dat Mitz ontworpen is als een centraal "policy decision point". Dat centraal ontworpen systeem zal bepalen welke gegevens gedeeld mogen worden. Het introduceert daarmee een centraal punt waarop hackers zich kunnen richten: een security hotspot.

Vernietigend oordeel NUTS

Op pagina 8 van de reactie staat een glashard oordeel dat ik u niet wil onthouden.

"De voorgestelde toestemmingsvoorziening legt dus heel veel macht in een centraal systeem en geeft vervolgens heel veel mensen schrijfrechten die onmiddellijk toegang moeten verschaffen tot medische data. We begrijpen de wens om bij een consult gegevens van een andere instelling in te kunnen zien. We begrijpen ook dat het wenselijk is om dan namens de patiënt een toestemming vast te kunnen leggen, zodat deze ontzorgd

wordt. Maar naar onze inschatting brengt het voorstel dat hier ter consultatie ligt een onacceptabel risico met zich mee op de vlakken van privacy en security.”

Tegenvoorstel

Op pagina 9 en 10 van de reactie van NUTS komt men tot een afgewogen tegenvoorstel. Daarbij wil men niet denken vanuit een specifiek product van een specifieke aanbieder maar vanuit een set aan gestandaardiseerde protocollen. NUTS stelt daarbij dat onderdeel van dat protocol zou moeten zijn dat toestemmingen om het beroepsgeheim te doorbreken worden opgeslagen in het systeem van de zorginstelling/-aanbieder die dat beroepsgeheim mag doorbreken. Een voorstel is een deel van die protocollen in het MedMij-stelsel onder te brengen.

Subsidiariteit/parlement/AP

Het stuk van NUTS maakt duidelijk dat de Mitz als online toestemmingsvoorziening niet proportioneel is. De gedachtegang van de mensen achter NUTS toont dat er als er gekeken wordt naar subsidiariteit(kan het ook anders en minder ingrijpend t.a.v. privacy en veiligheid) er zeer wel andere oplossingen te bedenken zijn voor de toestemmingsverlening voor de elektronische uitwisseling van zorgdata.

Terwijl de Tweede Kamer de gespecificeerde toestemming uitgebreid besprak, proberen ZN en VZVZ Mitz met medeweten en medewerking van VWS buitenparlementair te realiseren. Dat is op zijn zachtst gezegd niet alleen bijzonder vreemd, maar ook laakbaar. Nog vreemder is dat VZVZ in de nieuwsbrief van oktober 2020 doet voorkomen dat Mitz er gewoon komt terwijl er nog een open consultatieronde loopt.

Het is bovendien ook de hoogste tijd dat ook de Autoriteit Persoonsgegevens haar licht laat schijnen over het Mitz-voorstel dat alle Nederlanders betreft.

W.J. Jongejan, 5 oktober 2020