Regisseer de convergentie tussen de bestaande plateau-2-oplossingen in plaats van er parallel iets nieuws naast te ontwikkelen (steven van der Vegt, Nuts)

Algemeen

- Het daadwerkelijke probleem wordt niet opgelost: De werkgroepen Pull en Notified Pull kwamen niet tot eensgezindheid. (Jan-Joost van Walsum, UMCG, eerste paragraaf - Steven van der Vegt, Nuts, hoofdstuk 4, Gevraagd vervolg)

- Eerst in gesprek over het gelopen proces, de governance en vertegenwoordiging, de status van het document, de wijze waarop bestaande use-cases zijn betrokken en het beoogde vervolg. (Jeroen Bos, VZVZ, AORTA-LSP - Roald Dijkstra, Nedap)

- De beperkte scope moet duidelijk zijn, er moet geen voorschot genomen worden op daarbuiten liggende onderwerpen. (Steven van der Vegt, Nuts, hoofdstuk 2.3, alinea 2)
- Veel uitgangspunten zijn direct toepasbaar op alle uitwisselingssituaties. Het is wenselijk dit in versie 1.0 te verwerken. Dit is belangrijk voor het toekomstbeeld. (Jan-Joost van Walsum, UMCG, paragraaf 1 - Jonne Muilenberg, Twiin, Generieke toepassing - Ernst Lawende, Silizo, punt 7 - Roald Dijkstra, Nedap, alinea 4)

- Werk met een plateau-aanpak. Plateau 1 (push), plateau 2 (pull), target (Europese attestatie). (Steven van der Vegt, Nuts, hoofdstuk 4)
- Titel niet duidelijk betreffende reikwijdte en rede van bestaan. (Norbert van Dijk, RSO Nederland)

Juridisch

- NEN 7513 vereist dat uit de logging kan worden vastgesteld welke externe systemen gegevens hebben ontvangen. Modelleer de zorgaanbieder als vertegenwoordigende organisatie en het uitvoerende systeem als afzonderlijke oAuth-client. (Ernst Labende, Silizo, punt 2)
- Eist NEN 7513 herleidbaarheid naar de natuurlijke persoon die gegevens verwerkt en staat hiermee de oplossing op gespannen voet met de loggingsverplichtingen? (Jan-Joost van Walsum, UMCG)
- Het vertrouwensmodel mist de kaders voor een veronderstelde maatstaf voor toezicht. (Steven van der Vegt, Nuts, hoofdstuk 2.1)
- Kaderstellende partijen moeten per uitwisseling een risicoafweging documenteren, zoals bedoeld in hoofdstuk 5 en 6 van NEN-7512. (Steven van de Vegt, Nuts, hoofdstuk 1.1)
- Kaderstellende partijen moeten onderzoek doen en uitkomsten vastleggen over de (on)zekerheden van het gebruikte identificatiestelsel. (Steven van der Vegt, Nuts, hoofdstuk 1.1)
- Aansprakelijkheid achteraf vereist dat achteraf bewijsbaar is wie wat verklaarde. (Steven van der Vegt, Nuts, hoofdstuk 2.2)
- Deelname binnen het vertrouwensmodel is niet vaststelbaar. Er is geen register, lijst of verklaring waarmee dat kan. (Steven van der Vegt, Nuts, hoofdstuk 2.2)
- Voor logging over meerdere partijen heen is een correlatie nodig. (Steven van der Vegt, hoofdstuk 3.7)
- Ook de controle van de behandelrelatie moet vertrouwen op het federatieve vertrouwensstelsel. Hiervoor zijn binnen zorginstellingen al technische maatregelen ingericht. (Jan-Joost van Walsum, UMCG, laatste alinea)
- Is het inderdaad zo dat er geen persoonlijke identificatoren worden overgedragen van de bevragende zorgaanbieder naar de bronhoudende zorgaanbieder? Als dat inderdaad zo is, logt dan de bronhouder alleen de toegang van de aanvragende zorgaanbieder? Dan zou de bevragende zorgaanbieder de logging moeten bijhouden van wie van het eigen personeel externe informatie heeft geraadpleegd. Dit zou leiden tot aanpassing van de uitwisselsystemen;

de huidige logging is met name gericht op de toegang tot de brondata, en die ligt in dit geval niet bij de bevragende partij. (Jan-Joost van Walsum, UMCG)
- Op welke onderdelen geeft de voorgestelde oplossing invulling aan NEN 7512 en waar wijkt het juist af? (Jonne Muilenberg, Twiin)

Bedrijfsmatig / Beleid

Nu:
- URA afhankelijkheid en niet-zorgaanbieders buiten bereik (Steven van der Vegt, Nuts, hoofdstuk 3.5)

Voorstel voor nu:
- Er moet een grondige impactanalyse komen, zodat duidelijk wordt wat dit betekent. Door de korte reactietermijn was dit niet mogelijk. (Roald Dijkstra, Nedap alinea 1 - Jeroen Bos, VZVZ, AORTA-LSP, alinea 2 - Steven van der Vegt, Nuts, hoofdstuk 1)

Later:
- Een DPIA-handreiking opstellen om niet alle zorgaanbieders dezelfde analyse te laten uitvoeren. (Steven van der Vegt, Nuts, hoofdstuk 1.1)

Vragen:
- Waar landt dit memo besluitvormend en wat is de status van het concept na verwerking van de reacties; hoe verhoudt het memo zich tot de design authority en de bestaande architectuurgremia, en wie stelt het uiteindelijk vast; en komt er een nieuwe reviewronde op de verwerkte versie, met een termijn die impactanalyse en community-afstemming toelaat? (Steven van der Vegt, Nuts, hoofdstuk 1.1)
- Klopt het dat dit memo een basis op stelselniveau beschrijft en dat de kaders per uitwisseling nog volgen? Zo ja, wie stelt die op, en worden zorgaanbieders en standaardhouders daarbij betrokken? (Steven van der Vegt, Nuts, hoofdstuk 2.1)
- Ondanks de beperking in scope: is het de verwachting dat ook voor de overige uitwisselingen de autorisatie op zorgaanbiederniveau/organisatietypeniveau voldoende zal zijn en is dit daarmee het beoogde uitgangspunt voor alle autorisaties? Ik denk hierbij aan een UMC met een huisartsenpraktijk, een afdeling Psychiatrie en Revalidatie? Of betekent dit meerdere organisatietypes binnen een zorgaanbieder? (Jan-Joost van Walsum, UMCG, alinea 4)

Security

- Het huidige voorstel geeft onvoldoende invulling aan een zero-trustvertrouwensmodel. Mede door het verdwijnen van Verifiable Credentials. (Roald Dijkstra, Nedap, alinea 2)

Applicatie en technische architectuur

- NEN 7513 vereist dat uit de logging kan worden vastgesteld welke externe systemen gegevens hebben ontvangen. Modelleer de zorgaanbieder als vertegenwoordigende organisatie en het uitvoerende systeem als afzonderlijke oAuth-client. (Ernst Labende, Silizo, punt 2)
- Maak meer gebruik van aanwezige standaarden voor het gebruik van certificaten, bijvoorbeeld PKIo en UZI-certificaten met URA. Werk bijvoorbeeld met ondertekende delegatie (bijvoorbeeld mandaattokens). Gebruik geen URA voor ondertekening access tokens. (Vincent van den Berg, Chipsoft - Jonne Muilenberg, Twiin - Ernst Lawende, Silizo - Roald Dijkstra, Nedap - Steven van der Vegt, Nuts)
- Ga uit van een situatie met client registration. Introduceer oAuth Dynamic Client Registration voor de raadplegende SP. Er kan gewerkt worden met een allowlist. De wijze waarop authorization servers confidential clients en hun authenticatiemateriaal herkennen, is niet uitgewerkt. (Vincent van den Berg, Chipsoft - Ernst Lawende, Silizo)
- De keuze voor de client-credentialsgrant wordt ten onrechte met een verplichting uit FAPI 2.0 onderbouwd. Evalueer de keuze voor client-credentials en pas de motivatie aan. (Ernst Lawende, Silizo)
- Authorization_details is niet getekend. (Steven van der Vegt, Nuts, hoofdstuk 3.2)
- Self-asserted claims waar authentieke bronnen bestaan (Steven van der Vegt, Nuts, Hoofdstuk 3.4)

- Het autorisatiedeel is leeg (Steven van der Vegt, Nuts, hoofdstuk 3.6)
- Mag een zorgverlener-ID worden meegestuurd in de notificatie, de pullrequest, het access token of een bijbehorend authenticatie of autorisatiebewijs? (Jonne Muilenberg, twiin)