00:00:24  
*Maarten Swaap:* De datum is vandaag 25 oktober 2021. We spreken met elkaar in het kader van mijn master thesis en ik spreek met Geïnterviewde-03 van de Rijksdienst voor Identiteitsgegevens. Jouw functie is regie architect en dit gesprek is in het kader van mijn master onderzoek om te kijken of het gebruik van tokens en pseudoniemen ter vervanging van BSN. Dit zegt de titel, maar eigenlijk is meer een toevoeging van een extra unieke sleutel. Dit interview zou worden opgenomen in het Nederlands, de voertaal van de Nederlandse overheid, maar het zal worden vertaald naar het Engels voor de conclusies. De transcriptie zal ik bij je voorleggen en dan mag je van mij in snijden als je stukken hebt die ik echt niet mag opnemen, ook al staat je naam er niet boven. Want uiteindelijk zal de transscriptie zonder naam worden opgeslagen, de opnames worden gewist op uiterlijk 31 december en dat de transscriptie wordt bijgevoegd als documentatie bijlage bij mijn thesis. Ben je hiermee akkoord?

00:01:24  
*Geïnterviewde-03:* Ja, hier ben ik mee akkoord.

00:01:25  
*Maarten Swaap:* Mooi

00:01:26  
*Geïnterviewde-03:* Fijn om hieraan mee te kunnen werken. Om het echt even officieel te doen.

00:01:33  
*Maarten Swaap:* Leuk! Je rol en functie binnen RvIG is Regie Architect. Kan je kort introduceren wat je raakvlak is met het onderwerp? En wat je ervaring is.

00:01:46  
*Geïnterviewde-03:* Is zowel dat vanuit de technische achtergrond die ik heb opgebouwd. Met name in de realisatie rondom eIDAS. Daar ben ik toen ook wel mee bekend geworden, maar ook met de met de huidige encryptie cq cryptografische mogelijkheden, die gewoon geboden worden op dit moment. En daarnaast heeft het meer vanuit het domein, zeg maar is meer vanuit BSN domein en hoe daar uiteindelijk relaties mee leggen en dat soort zaken. Heeft het ook zeg maar meer een soort van een business waarde cq achtergrond op dat vlak.

00:02:30  
*Maarten Swaap:* Ja, want de business waarde waar je het over hebt. Ik heb eerder gezien dat vooral wat mijn onderzoeksvraag omschrijft is het alternatief voor BSN en wat ik eigenlijk zou willen oplossen is om te kijken om een stukje fraude te kunnen voorkomen. Dat is in twee opzichten: Eén is inderdaad niet meer kunnen koppelen van gegevens, dus dataset één en twee aan elkaar kunnen knopen [door middel van BSN]. Dat kan kan fraude opleveren, want met de set aan [persoons]gegevens, dan kun je in principe je voordoen als iemand anders. En ja, dat is eigenlijk het het het deel business waarde voor de burger. Wat ik zie, waarvan ik zou zeggen, daar zou ik willen op inzoomen nu om te kijken om een stukje framework te creëren hoe we technieken die daarbij kunnen helpen te toetsen. Dus dat is pseudonieseren en tokenizeren.

00:03:21  
*Geïnterviewde-03:* Er zitten voor mij qua business waarde zit dan nog een ander aspect zeg maar achter. Dat je juist dat je het technisch realiseert, er ook voor zorgen dat je van inzage mogelijkheid creëert. Dan kun je dat zowel actief als passief zeg maar doen. Dus in ieder geval dat je weet wat waarin gebruikt wordt en hoe de ketens uiteindelijk zitten. Vanuit business perspectief, maar vanuit de gebruiker cq. burgerperspectief is het ook zo dat je dus actief geïnformeerd kunt worden, dat als daar gebruik van gemaakt wordt. Want heel vaak gaat het, in ieder geval binnen de Nederlandse overheid vaak om die initiatie van een bepaald proces. En gaat het eens fout, vaak wat minder over de rest van de lifecyle. Als in het vergeten kunnen worden of kunnen verwijderen daarvan. Juist door die focus daar aan te geven is in mijn ogen de cirkel echt rond.

00:04:23  
*Maarten Swaap:* Ja, dus eigenlijk wat je zegt is dat ik als burger zou moeten kunnen zien als mijn gegevens worden gedeeld binnen de overheid of buiten de overheid, dat is even kort samengevat. Helder inderdaad

00:04:37  
*Geïnterviewde-03:* Dat kan, passief als ook actief zeg maar.

00:04:41  
*Maarten Swaap:* Ja, passief wil zeggen: iemand raadpleegt het zelf via MijnOverheid, of wat dan ook, en actief wil zeggen dat je iemand actief informeert: "Uw gegevens zijn gedeeld met partij x of y".

00:04:57  
*Geïnterviewde-03:* Ja, inderdaad.

00:04:58  
*Maarten Swaap:* Nou, ik eventjes kijken naar kwaliteitsattributen en daarvoor ga ik eventjes mijn scherm delen. Want het is eigenlijk kwaliteitsvereisten als we inzoomen en alternatieven schetsen voor een BSN nummer. Ik ga heel even kijken of ik mijn scherm kan delen. Dat kan ik natuurlijk en dat zal dan niet voor de opname [inzichtelijk] zijn. Staat ie hier, maar dan moet ik mijn mail tonen, maar dan moet ik mij.

00:05:27  
*Geïnterviewde-03:* Het andere scherm.

00:05:31  
*Maarten Swaap:* Deze inderdaad.

00:05:32  
*Geïnterviewde-03:* Ja, ja goed.

00:05:33  
*Maarten Swaap:* Wat we nu zien is een aantal kwaliteitsattributen die binnen ISO 25010 normering vallen. Als we kijken naar, als er een systeem optuigen. Ik noem het nu een systeem, maar als we kijken naar alternatieven sleutel voor BSN, dan is het de vraag: welke van deze kwaliteitsattributen zijn in jouw ogen belangrijk om rekening mee te houden?

00:06:02  
*Geïnterviewde-03:* Dat is allereerst. Ik begin even achteraan, is met name de portability en maintainability, waarbij de focus bij de overheden heel vaak bij maintainability uiteindelijk ligt. En eigenlijk één van de belangrijkste aspecten zou ik in deze op reliability uiteindelijk zetten.

00:06:31  
*Maarten Swaap:* Ja, reliability want die is in deze in deze context meer het systeem beschikbaar zijn, moet geen fouten in zitten er moet recovable zijn. Bedoel je dat met reliability of zit die meer op een ander aspect.

00:06:47  
*Geïnterviewde-03:* Om net één aspect, de reden eigenlijk: als in het gehele systeem heeft een bepaalde vertrouwenswaarde, zeg maar.

00:06:57  
*Maarten Swaap:* Ja

00:06:58  
*Geïnterviewde-03:* En dat, dat zie je een beetje dan in de maturity die juist door te laten zien van dat dit eigenlijk een als volwassene systeem zeg maar is dat je niet een Diginota 2 of zo hiermee gaat realiseren.

00:07:14  
*Maarten Swaap:* Wat je eigenlijk bedoeld is inderdaad een volwassen systeem. Gebruiker heeft ook het idee dat die, als ik het zo interpreteer, de gebruiker krijgt ook het idee dat ie een betrouwbaar overheidssysteem heeft. Wat...

00:07:25  
*Geïnterviewde-03:* Ja

00:07:26  
*Maarten Swaap:* goed met zijn gegevens omgaat.

00:07:28  
*Geïnterviewde-03:* Ja, dus ook een stukje transparantie zit daar uiteindelijk in die zit dan met name in mijn ogen aan de functional sustainability kant, zeg maar.

00:07:43  
*Maarten Swaap:* Ja, ja, die zit daar inderdaad in. Nou moet ik zeggen dat ik interpreteer functional sustainability en usability meer aan aan grafische interfaces (vooral usability).

00:07:56  
*Maarten Swaap:* Dus dat zou uiteindelijk belangrijk voor een eindoplossing zijn. Ik begrijp dat je functial sustainability zo opvatten zit het inderdaad in een correct [werkend] systeem, een compleet [werkend] systeem en dat soort zaken zit.

00:08:10  
*Geïnterviewde-03:* Wat je het eerste wat je zegt is dan eigenlijk ook als in functional completeness, dan zie je natuurlijk, wat ik net bijvoorbeeld ook zij, met inzage en collectie recht en dat soort zaken. Dan zie je al dat dat het meer over de levenscyclus gaat, hoe wordt uiteindelijk dan BSN uiteindelijk gebruikt? Welke de hele keten zijn het dan uiteindelijk? Dat je daar dus voor zorgt dat volledig is ingericht en dus ook gewoon transparant is ingericht.

00:08:42  
*Maarten Swaap:* Ja, want hoe zie je dat dan voor je? Dat op zich, want je zegt nu BSN en waar die gebruikt wordt in de keten. Als we natuurlijk uitgaan van een alternatief, zou die alternatieve sleutel worden gebruikt.

00:08:55  
*Geïnterviewde-03:* Wat je nou bijvoorbeeld kunt doen is dat je uiteindelijk op basis van je BSN kun je je identiteitsgegevens vragen en daar ook van opvragen hoe uiteindelijk die gegevens worden gebruikt. Datzelfde heb je natuurlijk ook rondom het alternatief hier uiteindelijk voor. Maar waarbij het alternatief natuurlijk gewoon vele malen groter domein uiteindelijk gaat worden. Dus daar zit, eigenlijk een soort van functionele vertaalslag tussen, want ik krijg eigenlijk dan inzicht hoe bijvoorbeeld de werking van DigiD is doordat daar eigenlijk gewoon die alternatieve BSN is ook intern binnen de systemen worden gebruikt. Kijk en dan weet ik veel beter eigenlijk van oké, maar zij doen een opvraging bij de BRP om de BSN en BRP gegevens om daarbij te halen. Is Geïnterviewde-03 wel echt Geïnterviewde-03, 'geboren op' en dat soort zaken.

00:10:13  
*Maarten Swaap:* Ja, klopt dus eigenlijk wat je zegt. Wat we natuurlijk zouden kunnen zeggen. We hebben een alternatieve sleutel en ik zou het bijvoorbeeld een sheet met sleutels aan iemand kunnen sturen per post. En die kan je vervolgens zelf gaan uitgeven aan instanties en zeggen hier kan je mijn gegevens mee ophalen. Eigenlijk zou dat dan niet, dat zou dan natuurlijk het stuk traceability weghalen waarschijnlijk. Der zou een stukje uit die keten weggaan waar je nu eigenlijk zegt de BSN doen we het nu al. Als we gegevens verstrekken, dan moet dat herleidbaar zijn, dan moet dat vastgelegd zijn dat dat verstrekt is. En dat zou in iedere nieuwe situatie eigenlijk dezelfde situatie moeten zijn. Alleen als we natuurlijk zorgen dat gegevens veiliger worden gedeeld, zou het ook kunnen zijn dat het buiten de overheid of semi overheid gedeeld zou kunnen worden, waardoor je daarin grotere keten en meer partij zou hebben.

00:11:05  
*Geïnterviewde-03:* Ja, dat is één van de kantelingen zeg maar, dat is meer naar buiten toe geredeneerd als van het maakt dan eigenlijk niet meer uit. Dat is natuurlijk het nadeel van zo'n BSN alternatief. Dan blijf je eigenlijk wettelijk gezien binnen dezelfde grenzen. Maar, die kun je natuurlijk gewoon openbreken dat er op een gegeven moment een alternatief uiteindelijk is. Waarbij je dan niet meer te maken hebt met de wetgeving rondom de BSN alleen.

00:11:37  
*Maarten Swaap:* Ja.

00:11:39  
*Maarten Swaap:* Dit is misschien een zijstapje van deze kwaliteitsattributen. Zou je willen dat er het alternatief van BSN dat ene nummer of één cryptografisch nummer is die aan verschillende partijen wordt verstrekt. Of zou je in de ideale wereld zeggen. Ik heb hier voor iedere partij een andere sleutel of een andere token of een ander pseudoniem wat ik verstuur. Zodat, als het op straat komt te liggen, dat iemand de schuldig [van het lekken] aan kan wijze of dat je [het lekken] weer terug zou kunnen draaien.

00:12:08  
*Geïnterviewde-03:* Dat is altijd één van de lastigste afwegingen inderdaad. Daar zul je morgen met Erik ook wel in gesprek mee komen. Dat verwacht ik. Maar daar is eigenlijk altijd de afweging in van dat het wel traceerbaar uiteindelijk moet zijn. Maar dat je daar eigenlijk ook altijd de tweeweg kant in hebt.

00:12:34  
*Geïnterviewde-03:* Met de tweeweg kant bedoel ik eigenlijk van als je op een gegeven moment een sleutel uitgeeft zeg maar, dat een andere partij nog steeds diezelfde sleutel gebruikt. En dan val je dus toch weer in een bepaalde, daarnaast relationele kant. Dus vandaar ook steeds is gezegd: met name rondom die pseudonymen kant van dat is eigenlijk altijd een steeds wijzigend algoritme, waarbij steeds een nieuwe sleutel wordt uitgegeven. Zodat in ieder geval tussen de twee partijen altijd bekend is om wie het uiteindelijk gaat, maar dat een derde partij daar alsnog gewoon niet bij kan komen.

00:13:13  
*Maarten Swaap:* Dus dat als mijn gegevens worden gedeeld met mijn pensioenuitvoerder dan zou dat een andere sleutel zijn dat mijn gegevens worden uitgewisselde met de belastingdienst.

00:13:26  
*Geïnterviewde-03:* Ja, transactionele verwerking. De micro verwerking eigenlijk. Is altijd een slag tussen twee partijen. Die kan altijd anders worden verpakt cq worden ingepakt. Als je dat even als principe hanteert ja, volgens mij heb je dan zeg maar de ultieme inrichting voor hoe we het veilig zouden kunnen doen.

00:13:55  
*Maarten Swaap:* Ja, ik heb een aantal stukken van hem [Eric Verheul] gelezen. Inderdaad ga ik morgen met hem in gesprek. Het is inderdaad, als ik het zo beluister, idealiter heb je inderdaad voor eigenlijk bijna iedere transactie zou je dezelfde uitkomst willen: een pseudoniem die herleidbaar is naar dezelfde persoon. Maar eigenlijk, als je het pseudoniem zou beetpakken en zou bekijken, zou dat eigenlijk idealiter er anders uitzien dan datgene wat je vorige week heb verstuurd aan dezelfde partij misschien.

00:14:23  
*Geïnterviewde-03:* Daarom is hij op een gegeven moment toen begonnen met Polymorfe Pseudoniemen. Dus die daar eigenlijk altijd, in deze dan, vaak tijds gebaseerd. Maar in mijn ogen is dat gewoon transactie gebaseerd. Als in van iedere keer dat een aanroep cq. transactie tussen twee partijen plaatsvindt dan moet dat in mijn ogen altijd een wijzigend iets zijn.

00:14:46  
*Maarten Swaap:* Ja, helder inderdaad. Als we kijken naar de kwaliteit vereisten. Dingen die je benoemde is natuurlijk een stukje Betrouwbaarheid. Hoe zou je de betrouwbaarheid kunnen meten? Misschien hele moeilijke vraag die ik stel.

00:15:06  
*Geïnterviewde-03:* Die kun je nu eigenlijk al meten, gezien de dienstverlening die daar gewoon achter zit. Welke eisen die dan stelt. Daar heb je de vroegere BSI indeling zeg maar van wat nou natuurlijk de ISO normering is. Als in één tot en met vier. Ik verwacht uiteindelijk dat daar nog wel meer granulair model gaat ontstaan. Want wat je nou bijvoorbeeld ziet is dat dat het hoogste niveau, zeg maar eigenlijk niet wordt gebruikt. En daar was dit nou net voor de ultieme toepassing. Terwijl ik denk van ja, maar het is eigenlijk wel onafhankelijk van welke dienst je dan eigenlijk hebt, dat je dat gewoon standaard aanbiedt.

00:16:03  
*Maarten Swaap:* Heb je voor mij, want je refereert aan de ISO normering, heb je die voor mij? Of weet je uit je hoofd welke dat is?

00:16:10  
*Geïnterviewde-03:* Die weet ik niet uit mijn hoofd. Inderdaad, ik zal hem achterhalen en even zoeken.

00:16:16  
*Maarten Swaap:* Of zit die toevallig in de eIDAS richtlijnen?

00:16:19  
*Geïnterviewde-03:* Inderdaad.

00:16:21  
*Maarten Swaap:* En dat betekent ook, de.....

00:16:26  
*Geïnterviewde-03:* De "levels off Assurance" zijn.

00:16:27  
*Maarten Swaap:* Inderdaad, en dat is de ja, ik snap wat je bedoelt. Dat is DigiD Hoog en dat soort zaken.

00:16:36  
*Geïnterviewde-03:* Daar zie je eigenlijk al fout in gaan in mijn ogen. Dat is omdat er op een gegeven moment een tijdelijk tussensituatie ontstaat waarin eigenlijk de lokale security levels gelijk moeten getrokken worden op Europees niveau. Terwijl in mijn ogen, ook het uitgangspunt is vooral een Level off Assurance van eIDAS in deze, die dan zeg maar even centraal stelt. Maar ik weet dat hier ook wel de ISO normering zeg maar achter hangt. Die weet ik dus even niet uit mijn hoofd.

00:17:16  
*Maarten Swaap:* Nee, oké, maar ik denk dat ik hem ook wel kan vinden en anders hebben we later even contact. Dat is wel een goede, want dat is dat is voor mij van de belangrijkste. Als die natuurlijk in de ISO normering valt en internationale gezien, de techniek geschikt is, dan ben je al een heel eind. Als iedereen het erover eens is dat dat dé techniek is. Als dat pseudoniemen zijn, dan zijn dat pseudoniemen. Als dat tokenizeren is, dan is dat tokeniseren, Als er een wat voor techniek dan andere ook is, dan is dat die andere techniek. Idealiter zou je zeggen, binnen dat raamwerk zou je toetsen of die voldoet. Ja, oké, ik weet niet of die toetsing al gedaan met een aantal techniek, maar het zou kunnen zoeken, natuurlijk, of je dat uit je hoofd weet.

00:18:00  
*Geïnterviewde-03:* Ja, die wordt in zoverre eigenlijk op de achtergrond gedaan. Als je een middel, zeg maar aanmeldt om te gaan gebruiken voor eIDAS. Wat je dan krijgt is dat andere landen eigenlijk een soort van onafhankelijke board vormen. Waarbij ze dan alle aspecten in ieder geval kijken van: Is dit dan inderdaad de juiste methode en kunnen we dus zeg maar koppelen?

00:18:35  
*Maarten Swaap:* Ja, en ik zie inderdaad een aantal peer reviews voorbij komen inderdaad. Dat er binnen Europa met een aantal experts op dat gebied wordt getoetst of het daadwerkelijk voldoet.

00:18:46  
*Geïnterviewde-03:* Ja, daar hebben we eigenlijk nog wel discussie over gehad. Natuurlijk wat je ziet is dat met name dit is in ieder geval toch een wat nieuwere techniek. Die we zo hebben vastgesteld dat Europa, stel dat Nederland eigenlijk het beste beentje voorzet vooroplopend op Europa en wetgeving. Daar zag je dus dat dat ook wel ons tegenwerkt. Omdat het kwaliteitsraamwerk is dan eigenlijk niet goed geschikt om die techniek van Polymorfe Pseudoniemen enzo, om dat ook goed te kunnen waarderen, zeg maar.

00:19:32  
*Maarten Swaap:* Er is dus eigenlijk, want dat is één van mijn volgende vragen, als we hier natuurlijk naar kijken: Wat zijn de zorgen die je hebt om, niet alleen technisch gezien, maar bij implementatie? Want als je nu zegt: ik heb dus inderdaad op basis van ISO normering en eIDAS normering weet ik wat de verschillende classificaties zijn, Level off assurance. Maar eigenlijk wat je hiermee zegt is dat de expertise en de manier van toetsen. Dat is volgens mij nog een uitdaging. Of zeg ik nu iets verkeerds?

00:20:04  
*Geïnterviewde-03:* Dat is echt een handje vol met mensen die er dan weten a la de Erik Verheuls en wat mensen die dan rondom BSN koppelregister hebben gewerkt. Met de HSMs, die dan weten welke er apps cq applets daarvoor is gebouwd zijn. Datzelfde geldt binnen de RvIG als in van dat is met een Anouk, maar dat ben ik zelf ook al een tijdje geweest. Dat je dan echt weet wat er op een gegeven moment echt over de lijn gaat, zeker moet en dat je daar dus ook gewoon zelf ook je test voor zou moeten schrijven. Dus het zijn niet meer de verschillende disciplines die je dan kunt vragen. Dus het is echt een handjevol mensen die daar gebruik van kan maken.

00:20:58  
*Maarten Swaap:* Ja.

00:20:59  
*Geïnterviewde-03:* Dat heb ik wel ook rondom cryptografie uiteindelijk gezegd. Al in van die gang zie je natuurlijk naar de cloud. Als in SaaSleveranciers en daar zul je gewoon veel meer cryptografie gaan toepassen. Maar dan heel specifiek voor dit alternatief, betekent dat eigenlijk, mag weer een veel kleinere subset van mensen die dat dan uiteindelijk weet. Daarvan heb ik ook al gesteld van laten we dat dan in ieder geval gewoon bundelen en in een soort van zijn Center of Excellence ofzo gaan organiseren. Dat zijn gewoon vanuit wiskundige perspectief, daar is natuurlijk ook gewoon nog steeds een doorontwikkeling in, maar dan heb je meer over de toepassingsgebieden bijvoorbeeld. Van hoe kun je dat dan uiteindelijk doen? Dat werkt natuurlijk twee kanten op. Als in van buiten naar binnen, van welke diensten zijn er dan die van die hoge niveaus gebruik willen maken? Tot aan de interne dienstverlening uiteindelijk. Want ja, je wil eigenlijk gewoon je hele dienstverlening eigenlijk gewoon, moet even BSN alternatief, agnostisch maken. Dus dat dat dat voor alle systemen wordt doorgeregeld [reusability].

00:22:23  
*Maarten Swaap:* Ja, wil dat technisch gezien in de hele keten dezelfde methodieken worden gebruikt?

00:22:29  
*Geïnterviewde-03:* Ja

00:22:29  
*Maarten Swaap:* Zodat je niet op allemaal verschillende plekken verschillende methoden hebt. Dat is één van die zorg en aandachtspunten als ik het zo mag vertalen.

00:22:35  
*Geïnterviewde-03:* Ja

00:22:35  
*Maarten Swaap:* Is dat je eigenlijk misschien dat ik het wiel op de ene plek uitvindt en iemand anders op een andere plek. En we doen misschien eigenlijk hetzelfde met een andere techniek, met een ander component en we doen eigenlijk gepseudonimiseerde we allebei ongeveer hetzelfde. Maar net op een andere manier, waardoor je het dan nodig vindt om met elkaar de discussie aan te gaan en naar elkaar uit te leggen. Ik zit ook even te denken. Ik kan me ook voorstellen dat een zorg is van hoe leg je dit uit aan stakeholders buiten RvIG en aan politiek, aan burgers, want ik kan me natuurlijk voorstellen dat ik ben nu aan het invreten in deze materie. Ik vind het als informatiekunde al heel ingewikkeld.

00:23:12  
*Geïnterviewde-03:* Mmm.

00:23:13  
*Maarten Swaap:* En hoe ik dit eruit zou moeten liggen aan iemand anders, ik zou het zelf niet zozeer weten. Nou, dus is dat ook een zorg die er is? Zie je die als zorg?

00:23:25  
*Geïnterviewde-03:* Die is zeker, want die is ook destijds wel aangekaart als in van communicatie moet richting de burger ook ontstaan. Vandaar is ook zeg maar het inzage register als dienst naar boven gekomen. Dan maak je het aan de ene kant transparantie, terwijl je aan de andere kant de technische aspecten gewoon niet hoeft te laten weten. Ja, je kunt natuurlijk gewoon op basis van universitaire onderzoeken en dat soort dingen kun je dat natuurlijk wel gestaafd krijgen. Dat dit gewoon even het juiste niveau is.

00:23:58  
*Maarten Swaap:* Dus eigenlijk zeg je....

00:24:00  
*Geïnterviewde-03:* Dus het maximaal haalbare. Maar richting de burger hoef je natuurlijk niet meteen het Polymorfe Pseudonyme algoritme uit te gaan leggen, want dan raak je ze toch gewoon kwijt. Maar wel dit is gewoon de facto standaard die op dit moment gebruikt wordt. En daar zitten deze waarborgen in, dan hebben we het voor jullie hebben we het op deze en deze wijze transparant gemaakt, zodat je in ieder geval kunt zien dat er ook gewoon echt een volwassene inrichting aan de ene kant is en een andere kan natuurlijk ook voor het gebruik ervoor zorgt dat je uiteindelijk. Daar is natuurlijk wel uiteindelijk om te doen, gewoon uiteindelijk, met minder identiteitsfraude uiteindelijk gewoon moet gaan realiseren moet gaan terugzien. Laten we het zo zeggen.

00:24:48  
*Maarten Swaap:* Ja, wat je zegt is de complexiteit van zo'n systeem en de gemiddelde burger hoeft het niet te weten. Maar om te voorkomen dat het een blackbox wordt en iemand denkt: hé, wat gebeurt er precies? Wil je transparantie geven tot op het niveau waar je in ieder geval zegt: dat moet de burger weten, minimaal en maximaal. Dus als er is ingelogd met DigiD dan moet je dat kunnen zien. Als er gegevens zijn, gedeeld met de pensioenuitvoerder dan uiteindelijk hij dat kan zien. En daarmee is diegene de zorg dat de burger of de politiek gaat denken: "Hé, wat gebeurt er precies? Want er worden allemaal gegevens encrypt en uitgewisseld. Dat is één grote blackbox!" Helder, oké. Even kijken, want ik kijk naar één vraag die ik nog heb: Van welke zorgen zijn nog actueel en moet de aandacht aan worden besteed als we een alternatief voor BSN implementeren. Dus oftewel: Welke openstaande puntjes zijn er nog?

00:25:43  
*Geïnterviewde-03:* Welke open eindjes zijn er dan nog...?

00:25:46  
*Geïnterviewde-03:* Dan kom je eigenlijk meer in: Hoe wordt het gebruikt uiteindelijk, die technieken? Dan zie je dat een aantal andere. Nou zeg je dat technieken die nog voor de communicatieve kant gebruikt worden, als in REST API's en dat soort dingen. Daar is het eigenlijk nog niet mee opgelost. Want je hebt dus je hebt maar dan de indeling van GET, PUT, POST en dat soort dingen. En eigenlijk wordt dan nog steeds van het gezegd dat als je zo'n pseudoniem zeg maar over de lijn stuurt, eigenlijk voldoet het dan nog steeds niet aan de standaard. Zijnde dat je in een GET geen identificerend gegevens meestuurt. Dus vandaar dat ik nog wel zoiets heb van in de périphérique met name op de integratie kant. Daar zitten nog wel wat uitdagingen als wat een losse eindjes zeg maar.

00:26:52  
*Maarten Swaap:* Bedoel je daarmee te zeggen dat als ik GET functie doe, nou bijvoorbeeld op de BRP en ik zou een pseudoniem terugkrijgen, dat volgens, ik weet niet is dat een wet of is dat meer een richtlijn vanuit de REST API. Dat daar geen persoonsgegevens in mogen staan, ook geen pseudoniemen?

00:27:09  
*Geïnterviewde-03:* Ja, die komen dus vanuit twee kanten eigenlijk. Meer de privacywetgeving zeg maar. En ook vanuit ja, hoe de die moet ik er dan ook wel even bij zoeken, vanuit de beveiligingskant van APIs. Daar heb ik destijds uitgehaald dat je in een in GET eigenlijk nooit geen identificerende gegevens zou moeten zetten.

00:27:49  
*Maarten Swaap:* Maar in een POST zou het wel mogen?

00:27:52  
*Geïnterviewde-03:* In en POST zou het wel weer mogen, omdat je daar dan weer op een andere wijze kunt inrichten. Dan ben je dus eigenlijk een afwijking aan doen. Ja, van je hoe zeg je dat, van je REST API.

00:28:06  
*Maarten Swaap:* Ja klopt, ik weet dat er wel patronen zijn, om dat op die manier in te richten, maar ik weet niet of het wenselijk is

00:28:12  
*Geïnterviewde-03:* Ja inderdaad.

00:28:16  
*Maarten Swaap:* Wat je bedoelt is inderdaad, de GPDR, het pseudonimiseren van persoonsgegevens mag ook, maar het blijven persoonsgegevens. Daarmee is het gelijk aan, kan nog steeds gerelateerd worden aan een natuurlijk persoon, dus er moet ook worden overwogen dat dit informatie is die te herleiden is naar een identificeerbaar natuurlijk, persoon. Recital 26. Mooie wet.

00:28:39  
*Maarten Swaap:* Dus dat is één van de zorgen die je daarin hebt, dat ook al zet je een pseudonym op de lijn. Dan zou je eigenlijk bijna niet kunnen voorkomen dat als iemand persoonsgegevens opvraagt moet je ze gaan geven. Dan zou je kunnen zeggen: pseudonymen verstrekken is beter dan de huidige situatie, waarbij de lijn misschien beveiligd is, maar de inhoud, het package, nog steeds gewoon uit plain tekst bestaat misschien.

00:29:03  
*Geïnterviewde-03:* Ja, één van de dingen die je wel realiseert in mijn ogen is. Dat blijft op zich wel nog steeds te herleiden. Maar dan heb je natuurlijk in de keten is het al beperkt tot je weet van het is één van beide partijen die er dan uiteindelijk mee aan de haal is gegaan. En dus vanuit dat perspectief is het wel te achterhalen, maar je zou liever gewoon een andere oplossing voor willen hebben.

00:29:36  
*Maarten Swaap:* Ja, dat is natuurlijk te lastig, want dan zou je dan zijn meer op een stuk tokenization terugkomen. Dat je iemand een token stuurt, wat moet die dan met die token? Dan moet ie alsnog met die token informatie ophalen? Of niet? Of zegt ie gewoon met die token, ik heb voldoende om te bepalen dat dit de juiste persoon is.

00:29:56  
*Geïnterviewde-03:* Dan ga je meer de SSI [Self Souverain Identity] kant inderdaad op, als van: Je weet waar de bron uiteindelijk is. De gezag houdende partij. Die geeft uiteindelijk alleen claims af. Dus daar gaat nooit geen data over de lijn, daar gaat alleen verificatie van gegevens over. Dus alle partijen worden dan ook naar de verschillende bronnen toe geleid. Dus er vindt nooit meer informatie uitwisseling plaats. Buiten het feit dat alleen die claims dan over de lijn gaan.

00:30:29  
*Maarten Swaap:* Ja, dat je zegt: is dit inderdaad degene die het is? Ja! En dan heb je een token om dat te bewijzen en daarmee is dat afgedaan. Het is wel, ik zit even te denken, want wat is het nadeel dat daaraan zit?

00:30:45  
*Geïnterviewde-03:* Het nadeel wat eraan zit, is het zijn allemaal complexiteit aanvullende technieken.

00:30:54  
*Maarten Swaap:* Bedoel je dat ermee dat het een grotere keten wordt en daarmee meer afhankelijkheid krijgt?

00:31:05  
*Geïnterviewde-03:* Kennis en competenties bijvoorbeeld, want als ik zie hoeveel of tenminste hoe weinig mensen er eigenlijk van SSI bijvoorbeeld afweten. Echt van de achterkant. Als ook van welke technische producten cq leveranciers zijn daar dan mee bezig en in hoeverre is dat wel of niet te vertrouwen? En dan in hoeverre is dan wel of niet open. En al dat soort dingen meer natuurlijk. En wat je ziet is van: In hoeverre is daar al wet en regelgeving voor? Dat natuurlijk ook gewoon nog steeds zwaar achter.

00:31:42  
*Maarten Swaap:* Ja, ik wou net zeggen. Het feit dat GDPR pseudoniemen benoemt is natuurlijk al een hele mooi aanknopingspunt om pseudoniemen toe te kunnen passen. Waar inderdaad andere technieken die misschien ook gangbaar kunnen zijn. Daar is de vraag: het moet wel in een wet terugkomen ergens voordat we kunnen gebruiken.

00:32:05  
*Geïnterviewde-03:* Eén van de principes die ik eigenlijk nog steeds aan het toetsen ben, is van de bron hoeft niks meer te versturen. Die krijgt alleen aanvragen binnen en je hoeft alleen of ja of nee te zeggen, of inderdaad van "dit is gecertificeerd". En de vraag die gesteld is dus dat klopt gewoon.

00:32:27  
*Maarten Swaap:* Ja dan praat je meer over verwijzingen?

00:32:29  
*Geïnterviewde-03:* Heel veel verwijzingen krijg je daar dan natuurlijk uiteindelijk naartoe, maar volgens hoef je dus nooit meer informatielevering te doen. Zoals wij dat dan nu kennen, als in dat je daar eigenlijk de technieken van Erik [Verheul, polymorfe pseudoniemen] zou toepassen. Want eigenlijk hoef je zo'n BSN dus niet te communiceren, want dat is inderdaad eigenlijk gewoon een BSN alternatief is dat gewoon geworden. Maar het is eigenlijk ook gewoon totaal betekenisloos. Dat is gewoon een token in die transactie geworden.

00:33:01  
*Maarten Swaap:* Ja, en op basis van die token kun je iets vragen en iets vaststellen. En dat is natuurlijk de ultieme situatie. Alleen wat je aangeeft is dat daar een zorg in zit in wetgeving en in complexiteit. Dat nu is het al een complex met pseudonimiseren, maar hebben we tenminste een wettelijke basis. Tokeniseren is een factor complexer waarschijnlijk. En we hebben nog geen wettelijke basis daarvoor. Waar je natuurlijk ook zou kunnen zeggen, is het een beetje een kip en ei verhaal. We kunnen natuurlijk ook zeggen: we gaan erover nadenken en POC'en een eind er op los. En dan gaan we de wetgever influisteren en dan over een jaar of vijf.

00:33:42  
*Geïnterviewde-03:* Zo moeten we het doen inderdaad.

00:33:44  
*Maarten Swaap:* Ja. Ik ga in ieder geval de opname beëindigen, want ik heb in ieder geval wat antwoorden op mijn vragen. Dan stop ik nu.