

Autorisatie

De Nuts specificaties beschrijven hoe systemen elkaar autoriseren om gegevens toegankelijk te maken. Deze autorisaties zijn een afgeleide van wettelijke grondslagen.

- [Autorisaties volgens Nuts](#)
- [Autorisatie en toestemmingen](#)
- [Het autorisatieverzoek](#)
- [Internationale standaarden](#)

Autorisaties volgens Nuts

Om gegevens te kunnen uitwisselen zullen twee (computer) systemen moeten samenwerken. Het bronsysteem zal daarbij het bevrogende systeem toegang moeten verlenen. Of er nu gebruikers bij betrokken zijn of niet, uiteindelijk zijn het systemen die de gegevens uit een database halen en op het scherm tonen.

Het geven van toegang tot gegevens is een binaire beslissing: wel of geen toegang. Actuele wetgeving ligt ten grondslag van deze beslissing. Om een brug te slaan naar de wetgeving is het [Authorization Credential](#) gespecificeerd. In de basis is het zo dat als een opvragend systeem een geldig autorisatie credential kan overhandigen aan het bronsysteem dat het bronsysteem dan toegang verleent.

Welke grondslag er toe heeft geleid dat het autorisatie credential is uitgegeven is voor de Nuts node niet van belang. De vertaling van grondslag naar autorisatie credential wordt ook niet binnen de Nuts node gedaan. Deze verantwoordelijkheid ligt bij het XIS/ECD of een ander systeem of voorziening.

De rol van de Nuts node

Een Nuts node is dus geen bron van wettelijke grondslagen voor gegevensuitwisseling. Een Nuts node zal er voor zorgen dat autorisatie credentials worden uitgegeven, ingetrokken en uitgewisseld. Deze functionaliteit wordt aangeboden via een API. Een ander systeem zal de API moeten gebruiken om credentials aan te maken.

Het uitwisselen van autorisatie credentials tussen nodes is van essentieel belang. De credentials volgen [Internationale standaarden](#) (W3C Verifiable Credentials) en deze standaarden dicteren dat credentials gebruikt worden vanuit een digitale wallet. De Nuts node is te zien als een *cloud wallet* voor de zorgorganisatie welke te gebruiken is door de aangesloten software.

Voorbeelden

Hieronder volgen een aantal illustratieve voorbeelden van hoe het XIS/ECD verantwoordelijk is voor het bijhouden van de wettelijke grondslag tot gegevensuitwisseling en dat de Nuts node alleen het onderliggende autorisatie credential uitwisselt.

Verpleegkundige overdracht

Bij de verpleegkundige overdracht wordt er vanuit het versturende systeem een workflow gestart. Het starten van deze workflow is het gevolg van een toestemmingsvraag aan de patiënt: "U wordt op verzoek overgedragen aan X". Bij verwijzingen is het zo dat de data het proces mag volgen. Het feit dat er een overdracht workflow aanwezig is in het verzendende systeem is dus een afschrift van een geldige grondslag. Het versturende systeem zal de Nuts node API aanroepen en autorisatie credentials aanmaken voor het ontvangende systeem. De Nuts node aan de versturende kant en ontvangende kant (onderdeel van het netwerk) wisselen dan automatisch het nieuwe credential uit. Wanneer een gebruiker in het ontvangende systeem gegevens gaat ophalen zal het credential uit de wallet worden gebruikt om toegang te krijgen.

Zorginzage huisarts/thuiszorg

In deze use case wordt aan de cliënt tijdens de intake gevraagd of de huisarts bij het thuiszorgdossier mag. Indien de cliënt instemt zal in het ECD worden vastgelegd dat dit akkoord is (eventueel met een ingescande PDF en natte handtekening). Het ECD zal de Nuts node API aanroepen om deze "papieren toestemming" om te zetten in een autorisatie credential. Indien de cliënt bij de thuiszorg aangeeft dat de huisarts niet langer bij de gegevens mag, dan zal het ECD de Nuts node moeten aanroepen om het credential in te trekken.

Autorisatie en toestemmingen

Nuts of Mitz? Beide dus...

Op de [vorige pagina](#) is te lezen wat een autorisatie volgens Nuts precies is. Toch zien we dat er vaak een vergelijking wordt gemaakt tussen Nuts en toestemmingsvoorzieningen. Deze vergelijking klopt niet. Nuts heeft juist een toestemmingsvoorziening nodig om de expliciete toestemming als grondslag om te zetten naar een autorisatie credential. Wat Nuts echter mogelijk maakt is dat het niet uitmaakt welke voorziening een zorgorganisatie gebruikt. Ook zorgt Nuts er voor dat twee zorgorganisaties niet dezelfde voorziening hoeven te gebruiken. Nuts zorgt er voor dat de onderliggende systemen eenduidiger toegang kunnen verlenen en maakt hiervoor gebruik van zorgonafhankelijke open internationale standaarden.

Bij het ontwerp van de Nuts specificaties staan privacy en security hoog in het vaandel. Door het ontbreken van een centrale index en door slim gebruik te maken van het [autorisatieverzoek](#) voorkomt Nuts overbevraging en privacy hotspots. De zorgorganisatie die de gegevens beheert is altijd eindverantwoordelijk voor de beveiliging van de gegevens en het waarborgen van de privacy. In het ontwerp van Nuts is dit ook technisch zo geborgd: een systeem dat als verwerker optreedt voor de zorgorganisatie moet de Nuts node API aanroepen om autorisatie credentials aan te maken.

Conclusie: een zorgorganisatie kan kiezen hoe het expliciete toestemmingen registreert, dit kan lokaal in het XIS/ECD, dit kan in een regio-platform of in Mitz. Zolang er een koppeling is tussen een toestemmingsvoorziening en een Nuts node onder de verwerkingsverantwoordelijkheid van de zorgorganisatie kan deze Nuts node gebruikt worden voor gegevensuitwisseling op basis van expliciete toestemming.

Het autorisatieverzoek

Een generieke expliciete toestemming is als grondslag niet te vertalen in autorisatie credentials. Er is sprake van een dergelijke toestemming wanneer een patiënt het goed vindt als zijn gegevens gedeeld worden met alle zorgorganisaties. Het uitgeven van autorisatie credentials voor alle zorgorganisaties zou gezien kunnen worden als *overbevraging*, daarnaast zou het aan alle zorgorganisaties tonen waar de patiënt zorg krijgt. Om deze situatie toch te kunnen ondersteunen wordt er binnen de Nuts specificaties gewerkt aan het **autorisatieverzoek**.

Een autorisatieverzoek wordt verstuurd door een opvragende partij aan een bronhouder om toegang te krijgen. De bronhouder kan het verzoek goedkeuren op basis van een toestemmingsvoorziening of andere grondslag. Dit kan volledig geautomatiseerd of door minimale interventie van een zorgprofessional.

Lokalisatie

Nuts kent geen centrale index van lokalisatiegegevens en is daardoor afhankelijk van het zorgproces. Dit hoeft geen belemmering te zijn en kan in sommige gevallen zelfs voordelig werken. Voordat een Nuts node een autorisatieverzoek kan versturen, moet deze eerst weten waarheen het verzoek gestuurd moet worden. De ontvanger van het verzoek, de bronhouder, kan op verschillende manieren gevonden worden:

- het wordt aan de patiënt gevraagd
- in het dossier staat de bronhouder vermeld
- door het zorgnetwork op te vragen bij andere bronnen

Het laatst genoemde punt kan een krachtige manier zijn om een zorgnetwork in kaart te brengen. Het wel of niet delen van een zorgorganisatie binnen een zorgnetwork is namelijk dan onderdeel van het dossier. Hoe meer zorgorganisaties er gevonden worden, aan hoe meer zorgorganisaties het autorisatieverzoek verstuurd kan worden.

Internationale standaarden

Omtrent autorisaties maakt Nuts gebruik van de volgende standaarden:

- [OpenID for Verifiable Credential Issuance](#). Specificaties omtrent het uitgeven/aanvragen van credentials.
- [OpenID for Verifiable Presentations](#). Het gebruik van Verifiable Presentations binnen OpenID connect.
- [OpenID SIOPv2](#). Self-signed identiteiten binnen OpenID Connect.
- [Status List 2021](#). Standaard voor het intrekken van credentials.
- [DIF Presentation Exchange](#). Een Query formaat voor het zoeken van credentials in een wallet.
- [W3C Verifiable credentials](#). Verifiable Credential/Presentation specificatie.

Naar deze specificaties wordt ook verwezen vanuit [The European Digital Identity Wallet Architecture and Reference Framework](#)