# Voorraadagenda Edukoppeling architectuur

Opgesteld: 12 september 2023

Landingsplek voor het Architectuurdocument is op Sharepoint/Teams: [Edukoppeling Team/Afspraak/Architectuur/WIP](https://365kennisnet.sharepoint.com/sites/onderzoekdiscussieforumEdustandaard/Gedeelde%20documenten/Forms/AllItems.aspx?csf=1&web=1&e=7MC35W&cid=b2d720f3%2D254e%2D4876%2D8dac%2Deb6b24a673ec&RootFolder=%2Fsites%2FonderzoekdiscussieforumEdustandaard%2FGedeelde%20documenten%2FAfspraak%2FArchitectuur%2FWIP&FolderCTID=0x01200043E17E49E117104DA837D4B794C17BDE).

Werkgroepoverleg op 5 september 2023 heeft de volgende voorraadagenda opgeleverd voor het opstellen van een nieuwe Edukoppeling architectuur. Het betreft onderwerpen waar we als werkgroep een conclusie over willen trekken (en aanraden aan de architectuurraad). De lijst is geprioriteerd op basis van commentaar in het conceptdocument én aandachtspunten geïnventariseerd in de werkgroep.

1. Aanscherpen definities mandaat/consent/autorisatie

Deze woorden duiken regelmatig op, als het gaat om toestemming, maar hoe ze verband met elkaar? Het voorliggende architectuurdocument doet een aanzet:

* Mandaat/consent

Een mandaat, synoniem met consent, is de toestemming aan een SAAS-leverancier om namens een eindorganisatie te handelen voor een bepaalde dienstverlening.

[GGR: Een SAAS-leverancier identificeert en authenticeert leverancier zich met PKIO. De SAAS-leverancier kan services afnemen en aanbieden. Als hij afneemt identificeert hij in de aanvraag de eindorganisatie voor wie hij dat doet. Als hij aanbiedt verwacht hij dat de aanvrager in de aanvraag de eindorganisatie identificeert. Deze relaties moeten als mandaat bestaan.]

* Autorisatie

Een autorisatie is de toestemming aan een eindorganisatie om een dienst af nemen van een andere eindorganisatie, vaak het bevragen van bepaalde gegevens.

[GGR: Bij autorisatie gaat het om de vraag of de eindorganisatie (en indirect de SAS-leverancier) gerechtigd is om een specifieke service af te nemen].

Verwante vraagstuk: ROSA onderscheidt mandateringsvoorziening en serviceregister terwijl de omschrijving in beide gevallen duidt op leveranciers/dienstaanbieder van scholen én OSR componenten beide omvat. Hoe verhoudt zich dit tot het OAuth begrip “autorisatieserver” ?

1. Open/gesloten

Oorspronkelijk gaat Edukoppeling over vertrouwelijke gegevens. Later is deze specifieke scope losgelaten, maar heeft dat in de praktijk nog niet geleid tot een profiel voor de classificaties middel of laag. De huidige focus van Edukoppeling altijd gebleven bij “zware beveiliging” met PKI, TLS , Signing, Encryptie en Routering.

Persoonsgegevens zijn wettelijk gereguleerd door de AVG. Daarvoor moeten beveiligingsmaatregelen aanwezig zijn. Als het gaat om andere vertrouwelijke gegevens (bijv de normeringen in EDU-V of examenvragen van Facet) dan vallen deze onder dezelfde ‘zware beveiliging”.

Het voorliggende architectuurdocument heeft dit onderwerp nog niet geraakt. Voorstel opnemen in de tekst: Volg in alle gevallen de API-strategie van NL overheid: <https://docs.geostandaarden.nl/api/API-Strategie/> en volg bij vertrouwelijke uitwisselingen (één van de) bestaande Edukoppeling profielen. Die zijn urgent en belangrijk. Vooralsnog niet een eigen profiel voor vertrouwelijkheid laag. We onderscheiden vooralsnog geen aparte vertrouwelijkheidscategorie “middel”.

1. Verschillende toestemmingsvarianten

Doel van dit gespreksonderwerp is te komen tot een toestemming- of autorisatiemodel voor verschillende situaties. Een beslisboom. Voor de hand liggende variaties:

* + Toestemming met/zonder SAAS

Een onderwijsorganisatie én partijen als DUO moeten expliciete doelbinding hebben om met vertrouwelijke persoonsgegevens om te gaan. Een SAAS-leverancier doet dat op basis van een bewerkersovereenkomst en certificeringsschema.

Bijzonder geval, is toestemming van de leerling wel nodig als gegevens van de ene naar de andere gegevensverwerker (LAS. Leermiddel) worden overgeheveld? De onderwijsaanbieder heeft doelbinding en blijft verantwoordelijk.

* + Toestemming burger/onderwijsaanbieder

Een waarneembare trend is regie op gegevens waarbij de burger toestemming geeft aan een dienstverlener om gegevens van een andere dienstverlener te gebruiken. De zogenaamde eWallets zijn een potentiële geavanceerde vorm hiervan. De toekomst is misschien wel dat mensen niet meer inloggen bij een organisatie, maar organisaties bij een mens. Neemt de wg dit mee?

* + Toestemming 2 / 3 legged

Oauth ken een vorm waarbij de resourceowner in de autorisatieflow zit. Dat is de 3 legged variant. Die owner (medewerker van een onderwijsaanbieder) kan dan bijvoorbeeld online toestemming geven om een resource te gebruiken. In de andere oauth vorm, de 2 legged variant, is die toestemming vooraf gegeven en ergens opgeslagen in een register. Dit laatste type is centraal in de huidige Edukoppeling, maar dan zonder oauth. Overigens, er is nog een derde vorm: werken met een shared secret buiten de flow om, maar dat neem ik verder niet mee.

* + Toestemming één of twee stappen.

In het huidige Edukoppeling worden autorisatie en (eventueel) mandaat opgehaald uit een register. Het register staat in een vertrouwelijke omgeving waar de resourceowner moet inloggen. De bevraging van het register is zelf ook conform Edukoppeling.

Dit is vergelijkbaar met de Oauth 2 legged variant, alleen het resultaat is niet een levering van vertrouwelijke gegevens, maar een token. Er zijn qua inhoud twee opties:

* + - Token bevat OIN van de eindorganisatie

Het token bevat alle info die de resourceserver nodig heeft om tot levering over te gaan als het een geldig token is. Nadeel, zoals ondervonden door EDU-V: ze moeten voor elke onderwijsaanbieder een apart token aanvragen.

* + - Token bevat geen OIN van de eindorganisatie.

Door de eindorganisatie weg te laten is uit het token wordt geoptimaliseerd op het netwerkverkeer. Het is aan de resourceserver om alsnog de TO- en/of FROM te identificeren.

1. Onderwijsbreed of niet

Het werkingsgebied van Edukoppeling is nu omschreven als “het onderwijs”. Ik zou het nog wel wat scherper willen stellen: iedereen die samenwerkt met onderwijsinstellingen. In de praktijk zien we echter sectorale verschillen. Mijn stellingname: dat is niet nodig.

Edukoppeling maakt gebruikt van internationaal veel gebruikte frameworks. Soms is het lastig om op tijd nieuwe ontwikkelingen te omarmen, zoals bij REST en in ben benieuwd hoe met met GraphQL zal gaan, maar Edukoppeling heeft serieuze stappen gemaakt, nog voor Digikoppeling. Als een sector met een ander concept komt dan is het zaak voor de werkgroep om die te omarmen of bij te buigen.

De werkgroep rekent op de architectuur- en standaardisatieraad als richtinggevend en toeziendhoudend orgaan.

1. Legacy of niet

Deze versie van de architect rept op twee plekken over WUS of REST. In het ene geval gaat het een overzicht van de Edukoppeling – bestanden. Dat kan weg of veralgemeniseerd, Verder staat in paragraaf 4.4 voor een korte niet discutabele beschrijving. Opmerkingen van Erwin en Robert dat zij WUS als legacy zien en niet meer aan willen ontwikkelen. We hebben het er vaker over gehad en ik ben zeker voor een API-first principe. Ik vind dat nog te vroeg om WUS te staken. Het is een pas-toe-of-leg-uit standaard, er zijn een paar grote en dure toepassingen en ik sluit niet uit dat op het gebied van beveiliging nog doorontwikkeling nodig is. Transport en berichtbeveiliging met REST is denk ik nog niet op hetzelfde niveau. Ik vind het raar om in de architectuur niks te zeggen over WUS en REST maar wel daar nog een profiel voor te hebben (tot en met..).

1. OIN/BRIN/Routeringskenmerk/edu\_org\_id

Er is een apart Edukoppeling document over identificatie en authenticatie, maar helemaal eruit gekomen zijn we nog niet . Korte samenvatting:

* + We gebruiken OIN’s om organisaties te identificeren gebaseerd op RIO-BRIN of KVK
	+ We hopen al jaren dat we de stap naar onderwijsaanbieder-id’s kunnen maken, maar dat vlot niet.
	+ We onderkennen ook routeringskenmerken om aan te geven welke ‘tenant’ wordt gebruikt voor een bepaalde groep leerlingen.
	+ Dit speelt mogelijk ook een rol bij licenties voor leermiddelen (entitlement?)

Moeten we nog sleutelen aan de ontologie en dat opnemen in de architectuur?

1. Modernisering architectuur

Dit document stamt al vanaf 2013. Het is gemoderniseerd met requirements, maar het ontbeert nog typische architectuurhoofdstukken als Principes (b.v. API first) en Standaarden (b.v. Digikoppeling, API Strategie, NL GOV profiel)

1. Onder paraplu van Digikoppeling of niet

Digikoppeling is de moeder waarop Edukoppeling is gebaseerd. Vanaf het begin heeft Edustandaard een eigen ontwikkeling ingezet. EbMS was veel te moeilijk. Die trend zet zich door, REST is nog eens eenvoudiger. Daarin zijn we vooruitstrevend geweest en nog steeds denk ik. En met SAAS ook. Maar wel altijd in overleg met. Daarentegen, Digikoppeling is juist terughoudend om Edukoppeling- oplossingen te omarmen.

Maar met een beetje lenigheid kunnen we nog steeds zeggen dat onderwijsinstelling conform de (wettelijke) standaarden van het Forum Standaardisatie werken. Ik denk dat we dat moeten volhouden.

Ondertussen wordt er binnen Digikoppeling gekeken naar wat VNG/Common Ground/FSC/RINIS/NLX gebeurt. Ik kan dat nog niet goed op waarde schatten. Strategisch en financieel lijkt dit tamelijk stuurloos. Maar wel volgen.

1. Overige genoemde onderwerpen:
	* Inzage in toestemming: nut en noodzaak mij nog niet helder.
	* Logging: dit opgenomen bij requirement accountabililty.
	* Transport/berichtbeveiliging: Dit is al opgenomen bij requirements Security, div subrequirements.
	* Internationaal: als ‘eigen lijn’ in requirement Interoperabiliteit
	* OSR als concrete voorziening elders beschrijven?
	* Scenario’s, voorbeelden in het veld.
	* API-metadata (inhoud token, querystrings)