Edukoppeling

REST (best effort) profiel
voor
vertrouwelijke gegevensuitwisseling

Edustandaard

Datum: december 2019

Versie: 0.1

Status: concept

Inhoudsopgave

1. Historie

Versie	Auteur	Datum	Opmerking
0.1	E. Reinhoud	december 2019	Initiële versie

2. Inleiding

2.1. Aanleiding

Omdat gegevensuitwisseling meer en meer op basis van RESTful API's gerealiseerd wordt heeft de Architectuurraad gevraagd om een inventarisatie naar REST-standaarden uit te voeren om helder te krijgen hoe dit zich tot de WUS toepassingsgebieden verhoudt en wat nodig is voor een veilige en betrouwbare gegevensuitwisseling op basis van RESTful standaarden. Dit heeft geresulteerd in een Globale Architectuurschets (GAS[1]) welke vervolgens is gebruikt voor de ontwikkeling van een profiel voor ondertekenen en adresseren met REST[2]. Met dit profiel wordt beoogd om soortgelijke waarborgen voor integriteit, veiligheid en interoperabiliteit te bereiken zoals nu ook al beschikbaar is met het Edukoppeling WUS profiel met ondertekening van het bericht (2W-be-S). Voor dit profiel liep in de zomer van 2019 een openbare consultatie als onderdeel van het standaardisatieproces. In september zijn de resultaten hiervan besproken in de Edukoppeling werkgroep en is besloten het profiel in zijn huidige vorm niet als standaard aan de architectuurraad aan te bieden. Hiertoe is besloten om o.a. de volgende redenen:

- De technische invulling die wordt gegeven aan ondertekenen is een mogelijke variant, maar er zijn ook andere manieren mogelijk. Er is momenteel nog niet duidelijk wat het meest interoperabel is of gaat worden.
- De verwachting is dat bij toenemende behoefte voor het regelen van integriteit, onweerlegbaarheid, veiligheid en interoperabiliteit bij RESTful gegevensuitwisseling ook de standaarden hiervoor ontwikkeld worden. Het is wenselijk om aan te sluiten bij overheidsbrede keuzes en niet te snel een (deels) eigen ontwikkelde standaard te gebruiken die zeer waarschijnlijk niet gaat aansluiten bij deze overheidsbrede keuzes.
- Het ondertekenen maakt de implementatie complexer. RESTful gegevensuitwisseling wordt vaak gekenmerkt door een point-to-point koppeling waarbij er eerder niet dan wel noodzaak is om te ondertekenen.

De Edukopeling werkgroep heeft de architectuurraad aanbevolen om mogelijke afspraken voor RESTful gegevensuitwisselingen te inventariseren. Hierin wordt een point-to-point koppeling als uitgangspunt genomen. Op basis van het transportbeveiligingsprofiel (best effort profiel) wordt de integriteit en veiligheid van de gegevens in transport geborgd. Een ander uitgangspunt is dat het goed moet aansluiten op standaarden die overheidsbreed voor RESTful uitwisselingen voorgeschreven worden.

2.2. Doel en doelgroep

Deze versie van dit document is niet opgesteld met als doel om formeel vastgesteld te worden, maar wordt wel in de architectuurraad van januari 2020 besproken. We willen deze versie gebruiken om overwegingen inzichtelijk te maken en een gerichte discussie hierover te kunnen voeren. Hiertoe zijn ook expliciet een aantal aandachtspunten opgenomen. Op basis hiervan kunnen we in een volgende fase (tot zomer 2020) een formeel profiel ontwikkelen. Voorafgaand aan de vaststelling hiervan (in winter 2020) wordt het formele profiel eerst getoetst door verschillende ketens binnen de onderwijssector.

---

[1] https://www.edustandaard.nl/app/uploads/2018/12/Globale-Architectuurschets-GAS-REST-API-onderzoek-Edustandaard-1.0.pdf
[2] https://www.edustandaard.nl/app/uploads/2019/04/Ondertekenen-en-adresseren-in-REST-v0.5.pdf

2.3. Bronnen

1. Kennisplatform API's (API strategie) https://geonovum.github.io/KP-APIs/
2. Digikoppeling https://www.logius.nl/diensten/digikoppeling/documentatie
3. Edukoppeling https://www.edustandaard.nl/standaard_afspraken/edukoppeling-transactiestandaard/
4. OWASP https://www.owasp.org/index.php/OWASP_API_Security_Project
5. Verkenning API's https://www.logius.nl/sites/default/files/public/bestanden/diensten/DigiKoppeling/Overig/Verkennings%20API4GDI.pdf

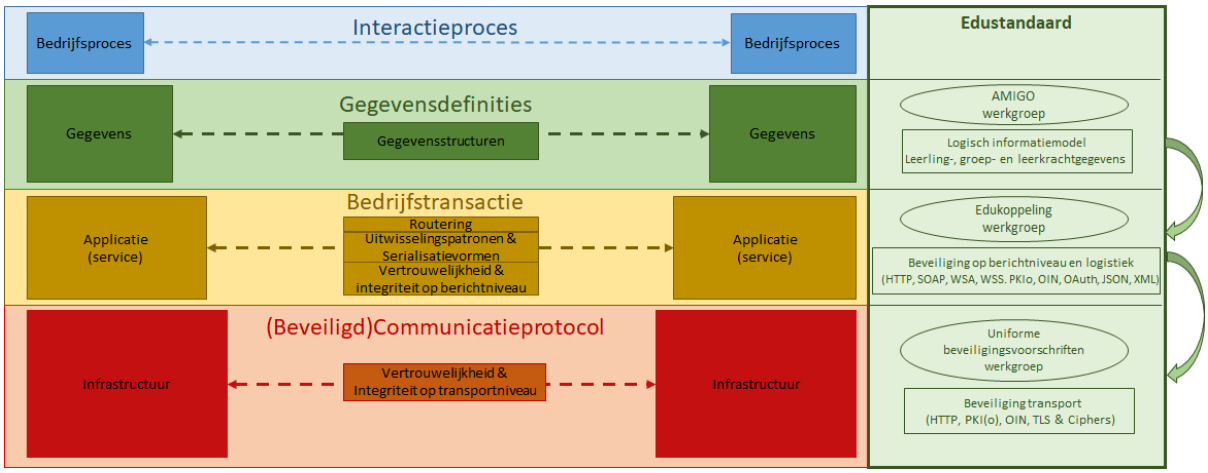
3. Aandachtspunten bij de ontwikkeling v/e REST profiel

Binnen het onderwijs zijn er al vele ketenpartijen die al RESTful gegevens uitwisselen. Deze ketens maken nu zelfstandig keuzes hoe transport, logistiek en beveiliging ingericht moeten worden. Voordat de concrete kaders van het REST profiel gedefinieerd worden, is het van belang eerst een aantal relevante aandachtspunten te beschouwen. Deze zorgen er voor dat we vooraf aan de opstelling van het profiel een beter beeld hebben van de te maken keuzes. Het betreft het volgende:

1. Scope Edustandaard werkgroepen
2. Standaarden en hun functioneel toepassingsgebied
3. Overheidsbrede REST afspraken
4. Overwegingen rond essentiële kenmerken v/e REST profiel

3.1. Scope Edustandaard werkgroepen

Er zijn verschillende Edustandaard werkgroepen die raakvlakken hebben met de standaardisatie van gegevensuitwisseling. Dit geldt met name voor de werkgroepen rond Edukoppeling, de Uniforme Beveiligingsvoorschriften en AMIGO. Het lijkt niet altijd evident wat de scope van een bepaalde werkgroep (standaard) is. Om te voorkomen dat werkgroepen vergelijkbare vraagstukken gaan oplossen is het wenselijk een duidelijke scope te definiëren en aan te geven hoe de verschillende standaarden elkaar aanvullen. We stellen voor om de scope van de werkgroepen in te richten zoals deze is weergegeven in Figuur 1.



Figuur 1 – Scope Edukoppeling werkgroepen

De Edukoppeling werkgroep ziet zich met name in het leven geroepen om de logistiek en beveiliging (Identificatie, authenticatie, ondertekening, versleuteling) rond gegevensuitwisseling te standaardiseren. Ook uitwisselingspatronen (AMIGO transactiepatronen) spelen hier een belangrijke rol (zie ook de Edukoppeling Architectuur[3]).

Hoewel dus ook beveiliging op transportniveau onderdeel is van de huidige Edukoppeling standaard, is ervoor gekozen om hiervoor een breder bereik te creëren dan alleen Edukoppeling implementaties. De voorschriften en het beheer hiervan zijn daarom overgedragen aan de werkgroep Uniforme beveiligingsvoorschriften.

[3] https://www.edustandaard.nl/app/uploads/2019/02/2019-01-31-Edukoppeling-Architectuur-1.2.2-definitief.pdf

Ondertussen is ook de Architectuur voor Modulair opgebouwde Interacties en Gegevensstructuren in het Onderwijs (AMIGO) in ontwikkeling. Hierin is naast het logisch informatiemodel ook een aantal uitwisselingspatronen opgenomen. Er wordt hierin tevens aangegeven dat push-berichten in principe niet zijn toegestaan (push-berichten worden in Edukoppeling toegestaan).

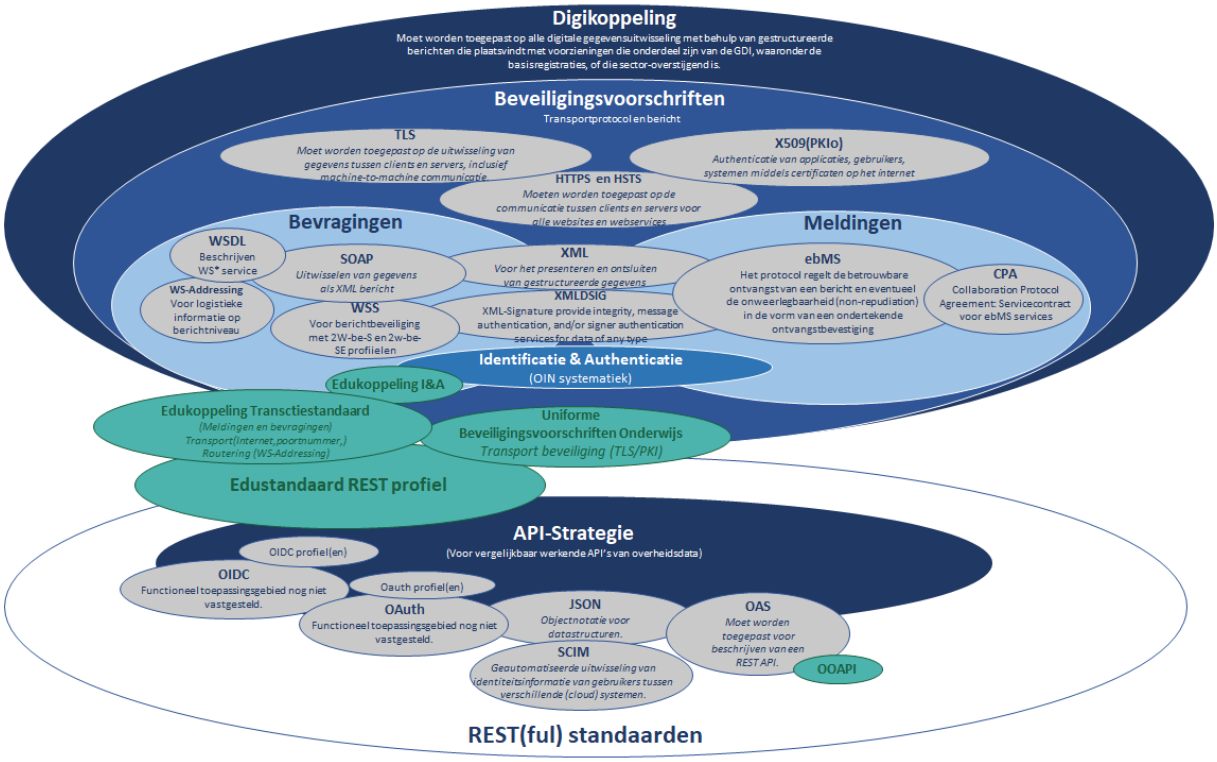
Zonder een duidelijk scope voor de verschillende werkgroepen kan er bijvoorbeeld de situatie ontstaan dat de Uniforme beveiligingsvoorschriften werkgroep het logisch vindt dat er een OAuth profiel voorgeschreven moet worden om in bepaalde situaties dit als aanvullende beveiligingsmaatregel voor te schrijven. Verder stelt AMIGO (versie 0.9) dus dat push-berichten in principe niet zijn toegestaan. De AMIGO werkgroep zou in een volgende versie ook kunnen overwegen om de OAuth uitwisselingspatronen op te nemen. En ondertussen zou de Edukoppeling werkgroep verder kunnen gaan met een REST profiel dat OAuth ondersteund. In Figuur 1 wordt een mogelijk indeling voorgesteld om te voorkomen dat werkgroepen parallel aan dezelfde vraagstukken werken.

3.2. Standaarden en hun functioneel toepassingsgebied

Er worden verschillende standaarden binnen de onderwijssector gebruikt met bepaalde functionele toepassings- en werkingsgebieden, maar het is niet altijd duidelijk welke dit zijn. In dat geval kunnen ketens zelf keuzes maken in welke situatie een bepaalde standaard toegepast gaat worden. Dit kan discussies opleveren en het is daarom wenselijk om een overzicht te hebben van de toepassings- en werkingsgebieden van standaarden.

Momenteel zijn de toepassingsgebied van Edukoppeling (Digikoppeling) redelijk in kaart gebracht. Dit is veel minder het geval voor RESTful standaarden. Het gedachtegoed van REST en de ontwikkeling van RESTful standaarden reiken ver en kan grote impact hebben op de huidige inrichting van de informatievoorziening. De toepassingsgebieden van RESTful standaarden zullen op termijn duidelijk worden, maar het is wenselijk om voor dit REST profiel nu al een toepassinggebied te definiëren. We stellen voor om dit profiel (voorlopig) te laten overlappen met het huidige functionele toepassingsgebied van Edukoppeling WUS (best effort). Kantekening hierbij is wel dat we het REST gedachtengoed met dit profiel sterk inperken. Het wordt gebruikt voor vertrouwelijke gegevensuitwisseling met de aanvullende beperking dat dit specifiek voor point-to-point koppelingen geldt en geen onweerlegbaarheid ondersteund. Daarnaast wordt het gebruik van het transportbeveiligingsprofiel van de Uniforme beveiligingsvoorschriften verplicht gesteld voor dit profiel. Dit is het uitgangspunt voor deze versie, maar we houden er rekening mee dat de inzichten die we de komende tijd nog opdoen er toe kunnen leiden dat er andere keuzes worden gemaakt.

Het expliciet aangeven dat er overlap is in het functionele toepassingsgebied stellen we eigenlijk dat we met een migratiefase te maken hebben. De WUS standaarden worden minder goed ondersteund in ontwikkelomgevingen en de huidige generatie ontwikkelaars heeft een voorkeur voor REST implementaties. Om zowel REST als WUS in hetzelfde toepassingsgebied mogelijk te maken wordt een apart beveiligingsprofiel voor transport als randvoorwaardelijk gezien. Met de Uniforme beveiligingsvoorschriften als basis kunnen hier bovenop de verschillende vormen van bedrijfstransacties toegepast worden (zie ook Figuur 1).



Figuur 2 – Overzicht functioneel toepassingsgebied standaarden en hun onderlinge afhankelijkheden

3.2.1. Digikoppeling

Digikoppeling moet worden toegepast op alle digitale gegevensuitwisseling met behulp van gestructureerde berichten die plaatsvindt met voorzieningen die onderdeel zijn van de GDI, waaronder de basisregistraties, of die sector-overstijgend is. Geautomatiseerde gegevensuitwisseling tussen informatiesystemen op basis van NEN3610 is uitgesloten van het functioneel toepassingsgebied.

Digikoppeling onderkent twee hoofdvormen van berichtenverkeer[4]:

- **Bevragingen**: een vraag waar direct een reactie op wordt verwacht. Hierbij is snelheid van afleveren belangrijk. Als een service niet beschikbaar is, dan hoeft de vraag niet als onderdeel van het protocol opnieuw worden aangeboden.
- **Meldingen**: men levert een bericht en pas (veel) later komt eventueel een reactie terug. In dat geval is snelheid van afleveren minder belangrijk. Als een partij even niet beschikbaar is om het bericht aan te nemen, dan is het juist wel gewenst dat het bericht nogmaals wordt aangeboden als onderdeel van het protocol.

Hoewel niet strikt voorgeschreven over het algemeen wordt het WUS protocol voor bevragingen gebruikt en ebMS voor meldingen of bevragingen.

[4] https://www.forumstandaardisatie.nl/standaard/digikoppeling

3.2.2. Edustandaard Edukoppeling

Edukoppeling is gebaseerd op Digikoppeling en het functionele toepassingsgebied van Edukoppeling komt dan ook overeen met die van Digikoppeling. Edukoppeling schrijft echter alleen het WUS protocol voor. Er wordt geen gebruik gemaakt van ebMS. De ROSA[5] stelt dat Edukoppeling gebruikt moet worden voor vertrouwelijke gegevensuitwisseling. Verder heeft Edukoppeling wel een ander werkingsgebied dan Digikoppeling, Edukoppeling wordt gebruikt binnen de onderwijssector.

Met Edukoppeling worden zowel bevragingen als meldingen ondersteund. Dit betekend dat er gegevens naar een service gestuurd kunnen worden (push), maar het voorgeschreven uitwisselingspatroon blijft hetzelfde (request-response). Indien er een betrouwbare overdracht gerealiseerd moet worden (zoals ebMS standaard ondersteund) dan zijn aanvullende afspraken nodig. De uitwisselingspatronen zijn beschreven in de Edukoppeling Architectuur[6].

Edukoppeling bevat een aantal wijzigingen op het Digikoppeling WUS protocol. Een belangrijk onderdeel is hiervan is het expliciet onderkennen van een SaaS leverancier en het hiernaar toe kunnen routeren door aanvullingen op de WS-Addressing voorschriften. Er worden drie rollen onderkent, een logistieke dienstverlener, een verwerker en een eindorganisatie. En SaaS leverancier is over het algemeen een gecombineerde rol van logistieke dienstverlener en verwerker. Op basis van de aanvulling op WS-Addressing kan deze de gegevensuitwisseling routeren naar de eindorganisatie (vaak een onderwijsinstelling). Verder heeft het net als Digikoppeling drie profielen, best effort voor point-to-point communicatie, een best effort profiel met ondertekening van het bericht om onweerlegbaarheid te ondersteunen en als laatste een best effort profiel met ondertekening en versleuteling van het bericht om gegevensuitwisseling via transparante intermediairs te ondersteunen. Een beveiligde point-to-point verbinding bestaat uit een tweezijdige TLS-tunnel om het verkeer tussen twee partijen in de keten te beveiligen. Hierbij wordt gebruik gemaakt van PKIoverheid certificaten met een Organisatie Identificerend Nummer (OIN) om de partijen te identificeren en authenticeren. Onderdeel van Edukoppeling is het Identificatie en Authenticatie document dat voorschriften bevat voor het OIN waarmee onderwijsinstellingen geïdentificeerd worden. De beveiligde point-to-point verbinding wordt nu nog in Edukoppeling beschreven, maar zal onderdeel worden van de uniforme beveiligingsvoorschriften. Edukoppeling zal hiernaar moeten gaan verwijzen voor transportbeveiliging.

3.2.3. Edustandaard uniforme beveiligingsvoorschriften

Edukoppeling wordt meer en meer toegepast bij uitwisselingen binnen het onderwijs, maar zeker nog niet overal. Als gevolg hiervan hebben partijen die in meerdere ketens bij gegevensuitwisselingen betrokken zijn, te maken met verschillende afspraken en de daarbij geldende beveiligingsvoorschriften. De uniforme beveiligingsvoorschriften worden onderhouden en sluiten aan bij bestaande voorschriften rond TLS, zoals de richtlijnen van het Nationaal Cyber Security Centrum (NCSC) waar ook de beveiligingsvoorschriften van Digikoppeling op gebaseerd zijn.

3.2.4. REST standaarden

Er is reeds een Edustandaard REST profiel, de afspraak Open Onderwijs API (OOAPI[7]). Het functionele toepassingsgebied is niet expliciet gedefinieerd, maar het betreft gegevensuitwisseling op basis van JSON en beschrijft de semantiek en syntax waaraan onderwijsinstellingen moeten voldoen om informatie beschikbaar te kunnen stellen aan externe partijen. Het werkgingsgebied is beperkt tot de HO sector en betreft processen waar o.a. persoonsgegevens, faculteitsgegevens, onderwijsafdelingen, onderwijsplannen, cursusgroepen, cursussen, cursusresultaten, toetsresultaten,

---

[5] https://www.wikixl.nl/wiki/rosa/index.php/Edukoppeling

[66] https://www.edustandaard.nl/app/uploads/2019/02/2019-01-31-Edukoppeling-Architectuur-1.2.2-definitief.pdf

[7] https://www.edustandaard.nl/standaard_afspraken/open-onderwijs-api/open-onderwijs-api/

gebouwen, ruimtes, roostergegevens, nieuwskanalen en nieuwsitems uitgewisseld worden. Hiermee heeft deze afspraak overlap met de voorschriften die een algemeen REST profiel gaat bevatten. De semantiek lijkt raakvlakken te hebben met wat in AMIGO[8] gedefinieerd wordt en de SCIM standaard. Dit hoeft geen probleem te zijn, de functionele toepassingsgebieden en werkingsgebieden kunnen verschillend zijn, maar het is nu niet duidelijk of dit zo is.

Voor REST in het algemeen is momenteel geen toepassingsgebied gedefinieerd. Wel zijn er een aantal relevante standaarden in de lijst van aanbevolen standaarden van Forum Standaardisatie opgenomen zoals OAuth[9] en OIDC[10]. Het is nog niet duidelijk of en in welke mate bepaalde REST standaarden gaan overlappen met het toepassingsgebied van Digikoppeling (Edukoppeling). In de API strategie staat wel een suggestie over het toepassingsgebied van OAuth[11]. Het ontbreken van het toepassingsgebied van REST standaarden leidt tot ongewenste discussies of ook RESTful standaarden gebruikt kunnen worden in het functionele toepassingsgebied van Digikoppeling/Edukoppeling.

3.3. Overwegingen rond kenmerken v/e REST profiel

3.3.1. REST profiel in perspectief van bredere ontwikkelingen

De huidige standaard (Digikoppeling/Edukoppeling) voor gegevensuitwisseling is ontwikkelt in de tijd dat voor B2B gegevensuitwisseling een servicegeoriënteerde architectuur (SOA) de de-facto standaard was. De uitwisseling werd gebaseerd op basis van een informatiemodel en gerealiseerd op basis van SOAP. De API werd gedefinieerd door een WSDL/XSD (of ebMS en een CPA). Tegenwoordig is de API een “product” geworden (zie Verkenning rond API’s[12]). De ontwikkeling van een API geschiedt op basis van een agile methode en er wordt niet meer uitgegaan van een informatiemodel, maar van user stories. API’s zijn in veel organisaties dè communicatievorm met de buitenwereld (en intern). De gegroeide behoefte aan ketenintegratie hoort bij het hyper-vernetwerkt zijn, het internet dat alles met elkaar verbindt. De noodzaak voor eenvoudiger integratie en de daaruit volgende standaardisatie zijn enorm gegroeid. Deze zichzelf versterkende cirkel heeft geleid tot “de API” zoals we die nu kennen en hun toepassing vinden we niet alleen op het web, maar als integraal onderdeel van applicaties op vele verschillende devices (IoT).

Dit profiel kent een zeer beperkte scope binnen al deze ontwikkelingen. We specificeren enkel een aantal aspecten om RESTful implementaties binnen het onderwijs te standaardiseren. Wel wordt de basis gevormd door het gedachtegoed van de REST architectuurstijl[13]. We gaan uit van resources en het gebruik van HTTP-methoden om deze te bevragen of te bewerken (level 2 volgens het Maturity Model van L. Richardson[14]). We maken zoveel mogelijk gebruik van bestaande standaarden om invulling te geven aan zaken als HTTP-methoden, schema's, foutafhandeling, versiebeheer en andere aspecten, maar de belangrijkste basis (in deze versie) zijn de transportbeveiligingsvoorschriften.

---

[8] https://www.edustandaard.nl/modulaire-architectuur-amigo-beschikbaar-voor-review/

[9] https://www.forumstandaardisatie.nl/standaard/oauth

[10] https://www.forumstandaardisatie.nl/standaard/oidc

[11] Functioneel toepassingsgebied OAuth: verplicht voor applicaties waarbij gebruikers (resource owner) toestemming geven (impliciet of expliciet) aan een dienst (van een derde) om namens hem toegang te krijgen tot specifieke gegevens via een RESTful API. Het gaat dan om een RESTful API waar de resource owner recht tot toegang heeft.

[12] https://www.logius.nl/sites/default/files/public/bestanden/diensten/DigiKoppeling/Overig/Verkennings%20API4GDI.pdf

[13] https://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm

[14] https://martinfowler.com/articles/richardsonMaturityModel.html

Binnen de onderwijssector bestaan nu al verschillende RESTful uitwisselingen, zoals Basispoort en het Onderwijs Service Register (OSR). Met dit profiel zorgen we ervoor dat deze en andere (toekomstige) B2B uitwisselingen waar persoonsgegevens RESTful uitgewisseld worden dezelfde transportbeveiligingsmaatregelen treffen. Conform Edukoppeling WUS gaan we nog steeds uit van clients die moeten kunnen beschikken over een API specificatie conform OAS (gebaseerd op een gestandaardiseerd informatiemodel) en deze roepen de API aan zoals voorgeschreven. De uitwisseling zelf is versleuteld met TLS en ketenpartijen hebben een overeenkomst rond de uit te wisselen gegevens en kunnen geïdentificeerd worden op basis van hun OIN. Naast de beveiligingsvoorschriften zijn er nog een aantal specifieke REST aspecten waarvoor we aansluiten op overheidsbrede afspraken (o.a. API-strategie).

3.3.2. De API-strategie als basis

Naast de transportbeveligingsvoorschriften vormt ook de API-strategie een belangrijke basis voor dit profiel. De API-strategie en overige producten van het kennisplatform API's[15] zijn in beheer genomen door Logius. Momenteel is er echter nog geen duidelijkheid hoe producten als de API-strategie binnen Logius gaan landen en op welke punten deze mogelijk nog gewijzigd gaat worden. Het is niet met zekerheid te stellen of de verschillende REST gerelateerde producten beheerd gaan worden in werkgroepen en of dit, meer specifiek het Technisch Overleg Digikoppeling gaat worden. Hoe het beheer ingericht gaat worden kan relevant zijn voor de mate van samenhang in afspraken rond REST en Digikoppeling. De keuze hierin is van belang voor het beheer van Edukoppeling documenten. Edukoppeling is momenteel volledig gebaseerd op gegevensuitwisseling op basis van het Digikoppeling WUS protocol. We verwachten dat eind voorjaar 2020 er meer duidelijk is hoe het beheer van de API-strategie ingericht gaat worden en hoe stabiel deze afspraken zijn. De belangrijkste principes uit de API-strategie zijn dan ook in dit profiel opgenomen zodat we een eigen oordeel kunnen vormen wat we van belang achten voor standaardisatie.

3.3.3. Uitwisselingspatronen conform Edukoppeling

Een belangrijke aspect binnen de REST architectuurstijl zijn de resources. Verder wordt het 'Gegevens bij de bron beheren' principe als een belangrijk onderdeel hiervan gezien. Het Common Ground[16] initiatief van de VNG stelt voor om efficiënter te gaan werken door één basisregistratie personen bij te houden, in plaats van gegevens heen en weer te schuiven van de ene lokale registratie naar de andere. Men wil gegevens niet meer van elkaar kopiëren om ze daarna zelf te beheren. In plaats daarvan worden API's gebruikt om gebeurtenis gedreven (informatie-arme) notificaties te sturen en worden gegevens zo veel mogelijk bij de bron beheerd. Dit gedachtegoed heeft impact op de noodzakelijke uitwisselingspatronen. Daarnaast wordt hiermee de ene organisatie van groot belang voor de continuïteit van de processen en/of diensten van een andere organisatie. Dit leidt weer tot de noodzakelijke afspraken over o.a. de beschikbaarheid.

We onderkennen dat dergelijke ontwikkelingen gaande zijn, maar binnen dit profiel gaan we er vanuit dat er (nog) meerde bronnen zijn voor dezelfde gegevens. Als gevolg hiervan stellen we dat we zowel te maken hebben met het bevragen van bepaalde bronnen, maar ook het synchroon houden van bronnen op andere locaties middels meldingen. We sluiten voorlopig aan op de uitwisselingspatronen zoals deze in de Edukoppeling Archtectuur[17] zijn gedefinieerd.

Bevraging (request-response)

---

[15] https://www.geonovum.nl/themas/kennisplatform-apis

[16] https://commonground.nl/

[17] https://www.edustandaard.nl/app/uploads/2019/02/2019-01-31-Edukoppeling-Architectuur-1.2.2-definitief.pdf

Het patroon request-reponse is het basale patroon waarbij een serviceprovider een webservice inricht, bijvoorbeeld voor het bevragen van een gegevensbron, waarbij de levering aan de servicerequester volgt binnen dezelfde sessie. Die wordt ook wel een synchrone uitwisseling genoemd.

Melding (request-response)
Het patroon melding-bevestiging lijkt op het vorige patroon. Het verschil is, dat de informatiestroom nu andersom loopt. De informatie wordt gestuurd door client en de ontvangst wordt synchroon door de service bevestigd. Het kan zijn dat deze bevestiging niet ontvangen wordt door de client en dat deze het bericht nogmaals stuurt. Hoe hiermee het beste omgegaan kan worden en of aanvullende voorschriften nodig zijn moet nog bepaald worden.

3.3.1. Opties om te kunnen routeren naar eindorganisatie

Het Edukoppeling WUS profiel ondersteunt het kunnen routeren naar een eindorganisatie op basis van de WS-Addressing (WSA[18]) standaard. In de WSA:From en WSA:To header wordt het OIN van de eindorganisatie opgenomen. We willen deze functionaliteit ook in dit profiel gaan ondersteunen door de identifier van de eindorganisatie mee te sturen. We onderkennen hiervoor nu de volgende opties:

- Opnemen als onderdeel van de URL (query parameter).
- Opnemen in een HTTP header
- Opnemen in een JWT

In deze versie kunnen we nog geen besluit nemen welke optie hiervoor het beste geschikt is. Verder kunnen er mogelijk ook nog andere opties geïdentificeerd worden. Concrete voorschriften rond routering worden in een volgende versie van dit profiel opgenomen.

3.3.2. Gebruik Onderwijs Serviceregister (OSR)

Momenteel kunnen (Edukoppeling WUS) services geregistreerd worden in het Onderwijs Serviceregister. Deze functioneert als een soort van “gouden gids” waarin partijen de endpoints van services van verschillende dienstaanbieders kunnen opzoeken. Onderwijsinstellingen hebben zelf services die ze willen registreren, maar het is vaak zo dat een onderwijsinstelling gebruikt maakt van de producten van een SaaS leverancier. Hierdoor zijn het niet meer de services van de onderwijsinstellingen die geregistreerd worden, maar de services van de SaaS leverancier. Het OSR onderkent deze situatie en ondersteunt tevens de functie om mandateringen te registreren. Het mandaat is de registratie dat een bepaalde leverancier namens een bepaalde onderwijsinstelling door middel van een service in een bepaalde context gegevens mag uitwisselen met ketenpartijen.

We gaan er vanuit dat de OSR functies ook voor RESTful API’s relevant zullen zijn. Dit heeft mogelijk wel consequenties voor het OSR en/of de API (de resources zullen afhankelijk van hun classificatie binnen de context van de mandatering moeten vallen). Of dit wenselijk is en hoe hiermee het beste omgegaan kan worden moet nog bepaald worden.

3.3.3. Geen verplichting voor OAuth

De API-strategie stelt als principe “Use OAuth 2.0 for authorisation” (API-14). Als invulling hiervoor is er een OAuth profiel[19] in ontwikkeling . Als functioneel toepassingsgebied wordt het volgende voorgesteld: “*Het gebruik van OAuth 2.0 is verplicht voor applicaties waarbij gebruikers (resource*

[18] https://www.w3.org/TR/ws-addr-core/
[19] https://geonovum.github.io/KP-APIs-OAuthNL/#dutch-government-assurance-profile-for-oauth-2-0

owner) toestemming geven (impliciet of expliciet) aan een dienst (van een derde) om namens hem toegang te krijgen tot specifieke gegevens via een RESTful API. Het gaat dan om een RESTful API waar de resource owner recht tot toegang heeft".

Het feit dat er momenteel nog geen profiel is vastgesteld door Forum Standaardisatie en het functionele toepassingsgebied ervoor zorgt dat er meer afgeweken wordt van het huidige toepassingsgebied van Edukoppeling WUS stellen we voor om OAuth nog geen verplicht onderdeel te maken van dit profiel. Op termijn zal OAuth zeker een belangrijke rol gaan spelen bij REST API's en onderdeel worden van een Edukoppeling REST profiel.

3.3.4. Focus op gesloten API's

Een organisatie heeft verschillende soorten API's[20]:

- Open API's: voor ontsluiten van diensten zonder toegangsbeperking bv open data.
- Gesloten API's: voor ontsluiten van diensten met toegangsbeperking bv persoonsgegevens en vertrouwelijke gegevens of diensten voor specifieke partijen.

Zoals bij het toepassingsgebied al is aangegeven is dit profiel bedoeld voor vertrouwelijke gegevensuitwisseling en betreft dus gesloten API's.

[20] https://geonovum.github.io/KP-APIs/API-strategie-algemeen/

4. REST profiel

4.1. Gebruikte methodiek bij prioritering (MoSCoW)

Per voorschrift wordt aangegeven hoe zwaar hier gevolg aan gegeven moet worden. Dit om duidelijk aan te geven wat de grenzen van het profiel zijn en waar men vrij is een eigen keuze te maken. Voorschriften worden aangeduid met Must, Should, Could en Won't zijn als volgt gedefinieerd:

- M – Must have: De Must have eisen moeten gerealiseerd worden. Hier kan niet van afgeweken worden.
- S – Should have: Implementatie conform voorschrift tenzij dit niet mogelijk is én er een work-around beschikbaar is die een vergelijkbaar resultaat mogelijk maakt.
- C – Could have: Dit betreft eisen die gewenst zijn maar waar men vrij is een andere keuze te maken.
- W – Won't have (this time): Deze eisen zijn (op termijn) wel gewenst maar voor nu is besloten deze functionaliteit niet verder uit te werken.

4.2. Uitgangspunten

Dit profiel heeft overlap met het functionele toepassingsgebied van Edukoppeling WUS. Het is specifiek voor point-to-point koppelingen en wordt gebruikt voor bevragingen en meldingen (push) op basis van een request-response uitwisselingspatroon.	
Rationale	De invulling van dit profiel is gericht op het gebruik van RESTful standaarden in hetzelfde toepassingsgebied als het Edukoppeling WUS best effort profiel. Voor beide kunnen dezelfde beveiligingsmaatregelen bij point-to-point transport voorgeschreven worden op basis van een UBV profiel. De Edukoppeling WUS profielen worden gebruikt bij uitwisseling op basis van XML.
Implicatie	Een REST API in de context van dit profiel wordt door de client altijd via een point-to-point koppeling op basis van JSON benaderd en is beveiligd met een UBV profiel. De client is in deze context geen browser, maar een systeem (applicatie). Als er sprake is van een transparante intermediair, de noodzaak voor onweerlegbaarheid, of gegevensuitwisseling op basis van XML dan wordt het Edukoppeling WUS profiel toegepast.

4.3. Afspraken

#1	**Must: De uitwisseling wordt beveiligd met een passend transportbeveiligings profiel zoals gedefinieerd in de uniforme beveiligingsvoorschriften (UBV)**
Rationale	In de huidige versie van de API-strategie beveiliging extensie (15-07-2019) worden al niet normatieve eisen minimaal TLS 1.3 en PKIoverheid voor access-restricted or purpose-limited API authentication voorgeschreven. De toepassing van dit profiel is expliciet gericht op access-restricted and purpose-limited API authentication. Hier wordt invulling aan gegeven door het UBV[21] transportbeveiligingsprofiel TLS & PKIoverheid(OIN). Dit is een basismaatregel om vertrouwelijkheid en integriteit tijdens transport te realiseren. Het UBV Tweezijdig TLS & PKIoverheid(OIN) profiel wordt nu al toegepast bij de toepassing van Edukoppeling WUS, zoals bij de BRON ketens. Het Programma van Eisen van PKIoverheid zorgt ervoor dat er voldoende betrouwbaarheid is rond de identiteit doordat wordt gecontroleerd of de aanvrager de tekenbevoegde van een organisatie is. Hierbij wordt een OIN gecreëerd op basis van de OIN systematiek en wordt opgenomen in het subject.serial van het certificaat.
Implicatie	Vooraf aan de uitwisseling wordt transportbeveiligingsprofiel conform het Edustandaard Uniforme Beveiligingsvoorschriften profiel ingericht. Dit profiel beschrijft de te nemen beveiligingsmaatregelen, zoals TLS versie(s) en ciphers. Er wordt verder aanbevolen om bedreigingen rond beschikbaarheid, integriteit en vertrouwelijkheid te beperken door het opvolgen van OWASP-richtlijnen[22].

[21] Er worden door de UBV nog twee profielen ondersteund. Dit zijn Enkelzijdig TLS: wordt bijvoorbeeld toegepast bij de ontsluiting van Linked Open Data) en tweezijdig TLS: wordt bijvoorbeeld toegepast als de client geïdentificeerd moet worden. Bij dit profiel maakt de keten zelf keuzes rond identificatie van de client en kan dus per keten verschillen.

[22] https://www.owasp.org/index.php/OWASP_API_Security_Project

#2	**De basis van dit profiel wordt gevormd door de overheidsbrede API-strategie[23] en extensies[24]**
Rationale	We sluiten aan op overheidsbrede afspraken (deze zijn nog wel in ontwikkeling).

[23] https://geonovum.github.io/KP-APIs/API-strategie-algemeen/ en https://geonovum.github.io/KP-APIs/API-strategie-extensies/ (15-07-2019)

[24] De extensies zijn nog in ontwikkeling, zie https://docs.geostandaarden.nl/api/API-Strategie-ext/

Implicatie	De API strategie[25] is nog niet formeel vastgesteld, maar is dus voor implementaties van dit profiel een belangrijke bron. De onderstaande kaders zijn uit de API strategie overgenomen. Indien er afwijkingen zijn dan zijn deze expliciet aangegeven. Aspecten rond tijdreizen en GEO-ondersteuning zijn in deze versie van het profiel niet overgenomen. API: • M: API-01: Operations are Safe and/or Idempotent • M: API-02: Do not maintain state at the server • M: API-03: Only apply default HTTP operations[26] • M: API-48: Leave off trailing slashes from API endpoints • M: API-04: Define interfaces in Dutch unless there is an official English glossary • M: API-05: Use plural nouns to indicate resources • M: API-06: Create relations of nested resources within the endpoint • M: API-09: Implement custom representation if supported • M: API-10: Implement operations that do not fit the CRUD model as sub-resources Documentatie: • M: API-16: Documentation conforms to OAS[27] v3.0 or newer • M: API-17: Publish documentation in Dutch unless there is existing documentation in English or there is an official English glossary available • M: API-18: Include a deprecation schedule when publishing API changes • C: API-51: Publish OAS at a base-URI in JSON-format Versioning[28]: • S: API-19: Allow for a (maximum) 1 year transition period to a new API version • S: API-20: Include only the major version number in the URI Extensie beveiliging[29]: • M: API-11: Encrypt connections using UBV profile Mutual TLS PKIo[30] • M: API-12: Access to an API is allowed if no API key is provided[31] • C: API-13: Accept tokens as HTTP headers only • C: API-14: OAuth 2.0 can be used for authorisation[32] • M: API-15: Use PKIoverheid certificates for API authentication (onderdeel van het UBV Mutual TLS PKIo profiel)[33] • C: API-49: Use public API-key's • C: API-50: Use CORS to control access[34] Extensie Versioning: • M: API-21: Inform users of a deprecated API actively Extensie JSON • M: API-22: IJSON first - APIs receive and send JSON • C: API-23: APIs may provide a JSON Schema • C: API-24: Support content negotiation • M: API-25: Check the Content-Type header settings • M: API-26: Define field names in in camelCase • M: API-27: Disable pretty print • M: API-28: Send a JSON-response without enclosing envelope • M: API-29: Support JSON-encoded POST, PUT, and PATCH payloads Extensie Filtering • M: API-30: Use query parameters corresponding to the queryable fields Extensie Sorting • M: API-31: Use the query parameter sorteer to sort

	Extensie Search • M: API-32: Use the query parameter zoek for full-text search Extensie Wildcards • M: API-33: Support both * and ? wildcard characters for full-text search APIs Extensie Paging • M: API-42: Use JSON+HAL with media type application/hal+json for pagination Extensie Caching • M: API-43: Apply caching to improve performance Extensie Rate limiting • M: API-44: Apply rate limiting • M: API-45: Provide rate limiting information Extensie Error handling • M: API-46: Use default error handling[35] • M: API-47: Use the required HTTP status codes

[25] https://docs.geostandaarden.nl/api/API-Strategie/ (15-07-2019)

[26] De HTTP HEAD, TRACE, OPTIONS en CONNECT operations are in the context of REST hardly ever used and have been excluded

[27] https://github.com/OAI/OpenAPI-Specification

[28] Er zijn richtlijnen voor versioning in API strategie opgenomen, maar geen principes

[29] De API strategie kenmerkt dit onderdeel als niet normatief

[30] We wijken af op de API strategie. De API strategie stelt: *Encrypt connections using at least TLS v1.3*

[31] We wijken af op de API strategie. De API strategie stelt: *Allow access to an API only if an API key is provided*

[32] We wijken af op de API strategie. De API strategie stelt: *Use OAuth 2.0 for authorisation.* In dit profiel wordt de toepassing van OAuth niet vereist. Dit wordt wel gezien als een essentieel onderdeel van een volgende versie. Deze zal waarschijnlijk gekoppeld zijn aan de profielen die Forum Standaardisatie vaststelt

[33] De API strategie beperkt de toepassing access-restricted or purpose-limited API's

[34] We wijken af op de API strategie, dit profiel gaat uit van communicatie tussen een client en server en er geldt geen verplichting.

[35] https://tools.ietf.org/html/rfc7807

5. Bijlage: Begrippen

Begrip	Uitleg
API	Het is een combinatie van technische bestanden (webservices), documentatie en andere ondersteuning die programmeurs helpen bij het aanroepen van externe applicaties/functies die zodoende in een website of platform geïntegreerd worden. Het zorgt daarmee voor gegevensuitwisseling tussen verschillende applicaties. REST staat voor REpresentational State Transfer, het is geen standaard of een protocol maar een architectuurconcept voor het aanspreken van services waarbij met name 'bruikbaarheid' centraal staat.
API-gewijze dienstverlening	Producten, diensten en stukken eigen taakuitvoering in de vorm van API's openstellen voor afnemers waarbij de API's als volwaardige producten gemanaged worden en een developer community een belangrijk aspect van de relatie met deze afnemers vormt.
API-strategie	Een bedrijfsstrategie gericht op het stap voor stap groeien naar API-gewijze dienstverlening die zowel de benodigde enterprise architectuur als organisatie en cultuurverandering omvat.
Beschikbaarheid	(Continuïteit) De mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ICT-dienstverlening waarborgen.
Integriteit	(Betrouwbaarheid) De mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.
Interface	Een interface is een technische koppeling tussen een systeem van een aanbieder en een systeem van een afnemer. Een interface is daarmee een implementatie van de semantische, syntactische en technische afspraken tussen partijen, de procesmatige afspraken worden meestal in een dienstverleningsovereenkomst / SLA vastgelegd. Een koppelvlak kan geïmplementeerd zijn door één of meerdere interfaces. Een interface wordt ook wel een service genoemd. Binnen het DSO onderkennen we twee categoriëen interfaces: Digikoppeling interfaces - bestaat uit koppelvlakstandaarden, die logistieke afspraken bevatten voor· berichtenuitwisseling tussen overheden. Application Programming Interfaces (API's) hebben als kerneigenschappen eenvoud, bruikbaarheid en· schaalbaarheid. Een API is een combinatie van technische bestanden, documentatie en andere ondersteuning. API's helpen programmeurs bij het aanroepen van externe applicaties/functies die zodoende in een website of platform geïntegreerd worden. Deze eigenschappen maken het mogelijk om data en diensten laagdrempelig beschikbaar te stellen en zoveel mogelijk gebruikers te bereiken.
JSON	JavaScript Object Notation, een formaat om net zoals XML gegevens op te slaan en te versturen. JSON kan ook gebruikt worden voor de inhoud van webservice berichten en is met name gericht op efficiënt programmeren. Kent een compacte notatie bijvoorbeeld: { "naam": Jan, "geboren": 1983 Zie https://tools.ietf.org/html/rfc7159
Koppelvlak	Een koppelvlak is een set van procesmatige, semantische, syntactische en technische afspraken tussen een aanbieder en afnemer die nodig zijn om de communicatie tussen twee partijen mogelijk te maken en goed te laten verlopen
OData	Toepassingsgebied: OData kan worden toegepast voor het bouwen en gebruiken van REST APIs met als doel het gestructureerd ontsluiten van (statistische) open datasets
REST	een architectuurconcept voor het aanspreken van webservices. Staat bekend om zijn snelheid en gebruiksvriendelijkheid. Meestal toegepast met standaarden als HTTP voor de transport en XML of JSON voor de berichtinhoud.

REST architectuur	REST is een architectuurconcept dat eind jaren 90 parallel met HTTP 1.1 is ontwikkeld door Roy Thomas Fielding[36] en gepubliceerd in 20009. De basis van REST is het interactie patroon van het web, geen toeval gezien de nauwe band met HTTP. Het beschrijft hoe interactie tussen componenten plaatsvindt in een gedistribueerd systeem. In de taal van het www: je hebt een webbrowser en een webserver, hoe praten die met elkaar? REST volgt dit zelfde interactie patroon van browser en webserver maar je client is geen persoon met een webbrowser maar een machine. In de praktijk wordt REST bijna altijd geïmplementeerd op basis van HTTP, maar dat is niet noodzakelijk.
Vertrouwelijkheid	(Exclusiviteit) De mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.

[36] Fielding, Roy Thomas (2000). "Chapter 5: Representational State Transfer (REST)".