edustandaard

# Memo

| | |
|---|---|
| Voor: | Architectuurraad, Edustandaard |
| Van: | Brian Dommisse (voorzitter werkgroep Edukoppeling) |
| Datum | 28-10-2019 |
| Betreft | Update opstellen REST-profiel: intrekken van huidige specificatie REST-profiel (versie 0.5) en advies voor het uitwerken van een best-effort profiel |

## 1. Gevolgd proces

Eind 2018 is in de werkgroep Edukoppeling geconstateerd dat de wijze van gegevensuitwisseling verandert. We hebben nu Edukoppeling WUS[1] profielen om een bericht op basis van best effort (point2point / Tweezijdig TLS), ondertekend, of ondertekend en versleuteld te versturen. 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) welke vervolgens is gebruikt voor de ontwikkeling van een profiel voor ondertekenen en adresseren met REST[2]. Met dit profiel werd beoogd om soortgelijke waarborgen voor integriteit, veiligheid en interoperabiliteit te bereiken zoals nu ook al beschikbaar is met de Edukoppeling WUS profielen.

De afgelopen periode is er een publieke consultatie uitgevoerd om de juistheid en toepasbaarheid van het profiel door partijen binnen en buiten de onderwijssector te laten toetsen. Hiervoor was onder meer een concept REST-profiel opgenomen binnen de Edukoppeling standaard en er is een post op het Edukoppeling discussieplatform[3] geplaatst. Bij de bespreking van de resultaten van de openbare consultatie binnen de werkgroep van 25 september 2019 is besloten dat het huidige profiel niet als standaard aan de Architectuurraad voorgelegd kan worden.

## 2. Onderbouwing besluitvorming[4]

Samengevat zijn voor de terugtrekking van het profiel dat ter consultatie voorlag (versie 0.5) de volgende argumenten aangevoerd:

- De kern van de specificatie van het REST-profiel zijn afspraken om representaties te ondertekenen ten behoeve van integriteit en onweerlegbaarheid. Deze aanpak lijkt op het WUS-profiel waarbij berichten ondertekend worden (zie discussieplatform[5]). Mede op basis van input vanuit de openbare consultatie

[1] https://www.logius.nl/diensten/digipoort/koppelvlakken/wus-voor-overheden
[2] https://www.edustandaard.nl/app/uploads/2019/04/Ondertekenen-en-adresseren-in-REST-v0.5.pdf
[3] https://groups.google.com/a/kennisnet.nl/forum/#!topic/edukoppeling/z52lTJS2Yhw
[4] De iets meer uitgebreide onderbouwing valt te lezen in het verslag van de Edukoppeling-werkgroep van 25 september 2019: 2019-09-25 Verslag Edustandaard Werkgroep Edukoppeling
[5] https://groups.google.com/a/kennisnet.nl/forum/#!topic/edukoppeling/z52lTJS2Yhw

wordt geconcludeerd dat om integriteit en onweerlegbaarheid te realiseren het meer voor de hand om de resources te ondertekenen.

- 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. Voor het standaardiseren van een REST-profiel met ondersteuning van integriteit en onweerlegbaarheid moet dit duidelijk zijn.
- 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. Het ondertekenen is met name wenselijk indien er transparante intermediairs in de keten zitten. Daarnaast zou het onweerlegbaarheid kunnen ondersteunen, maar met aanvullende ketenafspraken is dit minder noodzakelijk. Om dit met certificaten formeel te borgen moeten de certificaten hiervoor ook het juiste key usage ondersteunen.
- 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. Er lijkt nu (nog) geen acute behoefte. Overheidsbreed is men ook volop bezig met REST-implementaties en ook daar leeft de vraag om standaardisatie. 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.

## 3. Vervolgstappen

Er wordt wel onderkend door de werkgroep dat een REST-profiel als standaard wenselijk zou zijn binnen het onderwijsdomein. Daarbij acht de werkgroep dat er prioriteit moet worden gegeven aan een best effort profiel. Hierin wordt een point-to-point koppeling als uitgangspunt genomen waarmee op basis van een TLS koppeling de identiteit van de client wordt vastgesteld ten einde de integriteit en veiligheid voldoende te borgen. Een ander uitgangspunt voor het best effort profiel is dat het goed moet aansluiten op profielen en standaarden die onderwijs- dan wel overheidsbreed voorgeschreven (gaan) worden. Nadere afspraken dus over het toepassen van eenzijdig of tweezijdig TLS, het gebruik van PKIoverheid-certificaten etc.
Een dergelijk profiel zal waarschijnlijk eenvoudig zijn en voornamelijk voorzien in de informatiebehoefte om uniform REST API’s te definiëren. Voor de ontwikkeling van het best effort profiel zullen elementen uit de eerdere specificatie gebruikt worden. Daarnaast wil de werkgroep Edukoppeling kijken of in het basis best effort profiel adressering meegenomen kan worden om routering naar Edukoppeling rollen te ondersteunen of dat dit in een apart profiel opgenomen wordt.
Op de langere termijn bij voldoende behoefte zal er gekeken worden naar een profiel dat integriteit en onweerlegbaarheid bij verschillende use cases ondersteunt. Er zal dan ook gekeken worden of ook overige elementen uit het huidige profiel hierin opgenomen kunnen worden.

Kort gezegd komt het erop neer dat we adviseren om *bottom-up* te starten met markt- en overheidstandaarden en pas daarna, mocht het toch nog nodig blijken te zijn, uit te gaan breiden met moelijker te implementeren oplossingen.