Edukoppeling

REST/SaaS-profiel

voor

vertrouwelijke M2M gegevensuitwisseling

Edustandaard

Datum: maart 2020

Versie: 0.2

Status: concept

**Inhoudsopgave**

[1. Historie 3](#_Toc34837372)

[2. Inleiding 4](#_Toc34837373)

[2.1. Aanleiding 4](#_Toc34837374)

[2.2. Doel en doelgroep 4](#_Toc34837375)

[2.3. Positionering binnen Edukoppeling Architectuur 4](#_Toc34837376)

[2.4. Functioneel toepassingsgebied 5](#_Toc34837377)

[3. REST/SaaS-profiel 7](#_Toc34837378)

[3.1. Generieke voorschriften SaaS profielen 7](#_Toc34837379)

[3.1.1. Must: Gebruik van de UBV PKIo beveiligingsvoorschriften 7](#_Toc34837380)

[3.1.2. Must: Gebruik van openbare internet 8](#_Toc34837381)

[3.1.3. Must: Toegepast voor zowel bevragingen als meldingen 8](#_Toc34837382)

[3.1.4. Must: PKI infrastructuur 8](#_Toc34837383)

[3.1.5. Must: PKI-Overheidscertificaten 9](#_Toc34837384)

[3.1.6. Must: Identificatie & Authenticatie 9](#_Toc34837385)

[3.1.1. Must: Gebruik Onderwijs Serviceregister 10](#_Toc34837386)

[3.2. Specifieke voorschriften REST/SaaS-profiel 10](#_Toc34837387)

[3.2.1. Must: Routering o.b.v. (HTTP headerr/JWT) 10](#_Toc34837388)

[3.2.1. Should: Aansluiten op overheidsbrede afspraken rond REST 11](#_Toc34837389)

[4. Bijlage A: OAuth 13](#_Toc34837390)

[5. Bijlage B: Foutafhandeling (Authorisation errors) 14](#_Toc34837391)

# Historie

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Auteur** | **Datum** | **Opmerking** |
| 0.1 | E. Reinhoud | december 2019 | Initiële versie |
| 0.2 | E. Reinhoud | Maart 2020 | Aandachtspunten verwijderd, indeling generieke (overgenomen WUS) en specifieke voorschriften. Verschillende tekstuele wijzigingen |

# Inleiding

## 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. De inventarisatie en de ontwikkeling van een aantal concept profielen hebben uiteindelijk geresulteerd in het REST/SaaS-profiel dat in dit document is uitgewerkt. Hierbij worden een beveiligde point-to-point koppeling en het kunnen routeren tussen de Edukoppeling rollen als belangrijke uitgangspunten gehanteerd. Op basis van het transportbeveiligingsprofiel (op termijn UBV-voorschriften) wordt de integriteit en veiligheid van de gegevens in transport geborgd. Hierbij wordt de identiteit van beide partijen bepaald door het OIN in het certificaat dat wordt gebuikt voor de beveiliging van het transport. Een ander uitgangspunt voor dit REST/SaaS-profiel is dat het goed moet aansluiten op standaarden die overheidsbreed voor RESTful uitwisselingen voorgeschreven worden. De producten van het kennisplatform API’s worden daarom als basis gebruikt. De API Design rules en overige producten van het kennisplatform API’s[[1]](#footnote-1) worden in beheer genomen door Logius en zullen waarschijnlijk nog doorontwikkeld worden. We verwachten verder dat er in de nabije toekomst meerdere Edukoppeling REST-profielen zullen ontstaan voor andere contexten dan het SaaS-profiel.

## Doel en doelgroep

Dit document beschrijft de Edukoppeling REST/SaaS-profiel (verder aangeduid als REST-profiel) en is onderdeel van de Edukoppeling Architectuur. Het doel dat met dit profiel nagestreefd wordt is het op een generieke manier kunnen uitwisselen van gegevens binnen de onderwijssector. Daarbij wordt zowel het model waarbij een onderwijsinstelling zijn systeem zelf host, als waarbij de onderwijsinstelling deze via diensten afneemt van een SaaS-leverancier, ondersteund. Dit document definieert de kaders voor de profielen om dit te bereiken.

Dit document is bedoeld voor ICT-specialisten die betrokken zijn bij het ontwerpen en ontwikkelen van systeem-naar-systeem (M2M) koppelingen. Het gaat hierom werknemers (ontwikkelaars, architecten, projectmanagers, informatiemanagers etc.) werkzaam bij onderwijsgerelateerde organisaties, zowel in de publieke als private sector.

## Positionering binnen Edukoppeling Architectuur

Het Edukoppeling REST/SaaS-profiel is onderdeel van de Edukoppeling Architectuur. In het volgende hoofdstuk wordt het REST/SaaS-profiel inhoudelijk beschreven.



Figuur 1- Positionering van REST/SaaS-profiel binnen de Edukoppeling Architectuur

## Functioneel toepassingsgebied

Het functionele toepassingsgebied van het REST/SaaS-profiel betreft M2M-gegevensuitwisseling via een beveiligde point-to-point verbinding waarbij RESTful standaarden worden toegepast. Het wordt gebruikt voor bevragingen (pull) en meldingen (push) op basis van een request-response uitwisselingspatroon. De client is in deze context geen browser, maar een systeem (applicatie). Dit profiel heeft overlap met het functionele toepassingsgebied van het WUS/SaaS-profiel. De gegevens kunnen op basis van de afspraken binnen dit profiel gerouteerd worden tussen een verwerker en eindorganisatie. Dit laatste is geen verplichting indien de eindorganisatie ook de rol van verwerker (en logistieke dienstverlener) heeft. Als er sprake is van een transparante intermediair, of er is noodzaak voor onweerlegbaarheid, of gegevensuitwisseling op basis van XML dan wordt het Edukoppeling WUS-profiel toegepast.

Er is reeds een Edustandaard Open Onderwijs API (OOAPI[[2]](#footnote-2)) afspraak. Het functionele toepassingsgebied is niet expliciet gedefinieerd, maar ondersteunt processen waar o.a. persoonsgegevens, faculteitsgegevens, onderwijsafdelingen, onderwijsplannen, cursusgroepen, cursussen, cursusresultaten, toetsresultaten, gebouwen, ruimtes, roostergegevens, nieuwskanalen en nieuwsitems uitgewisseld worden. Het is nu nog niet duidelijk of hierin de Edukoppeling rollen expliciet onderkend worden en of het kunnen routeren hiertussen ondersteund wordt. Als dit het geval is dan is het wenselijk dat hierin dezelfde keuzes worden gemaakt. Omdat het werkgingsgebied beperkt is tot de HO-sector verwachten we niet dat er onduidelijkheid is wanneer welke afspraak toegepast moet worden.

Verder heeft ook de internationale standaard SCIM-standaard overlap met het functionele toepassingsgebied. Voor deze standaard kunnen we met zekerheid stellen dat de Edukoppeling rollen hierin niet expliciet onderkend worden en het kunnen routeren hiertussen.

Een organisatie heeft verschillende soorten API's[[3]](#footnote-3):

* 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 eerder aangegeven is dit profiel bedoeld voor vertrouwelijke gegevensuitwisseling en betreft dus gesloten API’s.

# REST/SaaS-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. Met dit profiel willen we hier meer standaardisatie in doorvoeren, waarbij we ook met name invulling willen geven aan het kunnen routeren tussen de rollen van het SaaS-profiel. We maken zoveel mogelijk gebruik van bestaande standaarden om hier invulling aan te geven.

Met 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 (pull) van bepaalde bronnen, maar ook het synchroon houden van bronnen op andere locaties middels meldingen (push). We sluiten hierbij aan op de uitwisselingspatronen zoals deze in de Edukoppeling Architectuur[[4]](#footnote-4) zijn gedefinieerd. Het profiel kan hierbinnen keuzes maken om bepaalde aspecten verder in te kaderen.

Voor het definiëren van dit profiel wordt er zoveel mogelijk aangesloten bij bestaande standaarden. We willen per voorschrift wel een bepaalde mate van ontkoppeling mogelijk maken en er is zodoende aangegeven hoe zwaar er aan een bepaald voorschrift gevolg moet worden gegeven. Hiermee kunnen we duidelijk aangeven wat de grenzen van dit profiel zijn t.o.v. de mogelijke externe bron waar het voorschrift van wordt overgenomen. Voorschriften zijn aangeduid met Must, Should, Could en Won’t waarvoor de volgende definities gelden:

* 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.

## Generieke voorschriften SaaS-profielen

### Must: Gebruik van de UBV PKIo beveiligingsvoorschriften

Voor beveiliging op transportniveau wordt gebruik gemaakt van de Edustandaard Uniforme Beveiligingsvoorschriften PKIo (UBV[[5]](#footnote-5)).

In de huidige versie van de API-strategie beveiliging extensie (15-07-2019) worden als 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[[6]](#footnote-6) 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, onder andere in de uitwisseling met BRON en Verzuim. 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.

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[[7]](#footnote-7).

### Must: Gebruik van openbare internet

De partijen die deel uitmaken van de sector onderwijs maken nagenoeg zonder uitzondering gebruik van het openbare internet om gegevens met elkaar uit te wisselen. Edukoppeling bevat maatregelen om beveiligde gegevensuitwisseling over een dergelijk openbaar netwerk mogelijk te maken. Overigens kan Edukoppeling, net als Digikoppeling, ook toegepast worden in gesloten netwerken.

### Must: Toegepast voor zowel bevragingen als meldingen

Voor betrouwbare gegevensoverdracht schrijft Edukoppeling een ander profiel voor dan Digikoppeling. Digikoppeling gebruikt hiervoor het ebMS-profiel. De onderwijssector wil geen complexe varianten introduceren die hetzelfde functionele doel hebben, maar biedt een architectuur die een end-to-end reliable interactieproces mogelijk maakt (in plaats van dit alleen op protocolniveau te regelen zoals Digikoppeling ebMS).

Betrouwbare gegevensoverdracht wordt vaak gekoppeld aan een melding, de initiator van de gegevensuitwisseling wil een andere partij informeren over een gegevenswijziging. De initiator verwacht niet direct een real-time resultaat, anders dan een bevestiging dat de gegevens zijn ontvangen. Op andere (business-)niveaus is het in deze context vaak wel gewenst dat de verwerking van de gegevens of aanverwante resultaten worden teruggekoppeld. Deze patronen kunnen zeer complex zijn en hiermee ook de standaarden die dit soort patronen ondersteunen. Edukoppeling beperkt zich daarom tot de Digikoppeling WUS-standaard, de 2W-be, 2W-be-S en de 2W-be-SE profielen voor synchrone communicatie. Deze profielen kunnen daar waar nodig aangevuld worden met Digikoppeling Grote Berichten-methodiek.

### Must: PKI infrastructuur

De koppelvlakken die bij de gegevensuitwisseling gebruikt worden en de gegevens zelf tijdens transport moeten voldoende beveiligd zijn. Conform Digikoppeling wordt hiervoor met een PKI-infrastructuur en certificaten gewerkt. Deze certificaten worden uitgegeven door Trust Service Providers(TSP). Een TSP is verantwoordelijk voor het controleren van de identiteit van de aanvrager en het opnemen van het identificerend gegeven dat voor deze aanvrager in het certificaat opgenomen moet worden. Edukoppeling schrijft conform Digikoppeling het gebruik van PKIoverheid-certificaten voor.

### Must: PKI-Overheidscertificaten

PKI-Overheidscertificaten zijn certificaten die worden uitgegeven in het kader van PKI-overheid van Logius. PKI-overheid certificaten hebben als root (mastercertificaat) ‘Staat der Nederlanden’ en zijn beveiligd naar de laatste stand van techniek. Zodra deze techniek niet meer voldoende is, zal er een nieuw type certificaat met een sterkere encryptiemethode gebruikt moeten worden. Uitgegeven certificaten hebben een beperkte geldigheidstermijn .

De certificaten worden uitgegeven door erkende TSP’s. De PKI-overheidscertificaten zijn van het niveau STORK4. Bij de uitgifte hoort ‘face-to-face’ controle: de houder neemt het certificaat persoonlijk in ontvangst. Het identificerend kenmerk wordt conform Digikoppeling systematiek bepaald (zie identificatie). De TSP die het certificaat uitgeeft heeft de verantwoordelijkheid om de uniciteit van het subject (service) te waarborgen en de identiteit te vermelden in het certificaat in het veld Subject.serialNumber.

Een Digikoppeling-certificaat is een specifiek PKI-overheidscertificaat. Bij de aanvraag hiervan moet men bij de TSP expliciet aangeven dat deze moet voldoen aan de specifieke Digikoppeling-eisen.

### Must: Identificatie & Authenticatie

#### Identificatie

Met een PKI-infrastructuur kan de identificatie en authenticatie van organisaties geregeld worden. Elke partij die via Edukoppeling de gegevensuitwisseling inricht, worden geïdentificeerd op basis van het unieke Overheids Identificatie Nummer (OIN), zie nummersystematiek Digikoppeling en het Edukoppeling Identificatie en Authenticatie document voor details. Voor onderwijsinstellingen is een prefix van 00000007 gereserveerd. Marktpartijen zullen over het algemeen de HRN-variant van de nummersystematiek toepassen (prefix 00000001 of 00000003). Hierbij worden de nummers vastgesteld door de TSP, op basis van het door de aanvrager opgegeven KvK-nummer, dat door de TSP wordt gecontroleerd.

Het zijn niet enkel de partijen die de verbinding voor de gegevensuitwisseling tot stand brengen die geïdentificeerd moeten worden, er zijn meerdere rollen te onderkennen. In de Edukoppeling Architectuur worden bij de gegevensuitwisseling de volgende rollen onderscheiden:

1. De eindorganisatie is de organisatie die in het kader van zijn doelstellingen samenwerkt met een andere organisatie.
2. De gegevensbewerker is een organisatie die in opdracht van de eindorganisatie gegevens verzamelt, opslaat, berekeningen uitvoert, verstrekt en dergelijke.
3. Een logistieke dienstverlener is een organisatie die faciliteert bij de verzending en ontvangst van berichten

(zie het Edukoppeling Architectuur document voor meer achtergrondinformatie).

Deze rollen worden op verschillende wijze geïdentificeerd. De eindorganisatie wordt geïdentificeerd middels de WS-Addressing To en From headers. De gegevensbewerker ondertekent het bericht met een XML-signature (op basis van een eigen PKI-certificaat met OIN). De logistieke dienstverleners kunnen middels de TLS-verbinding geïdentificeerd worden op basis van het PKIoverheid-certificaat wat hierbij gebruikt is.

#### Authenticatie

Bij authenticatie wordt een aangegeven identiteit geverifieerd. De mate van betrouwbaarheid kan hierbij verschillen. Authenticatie levert als het ware de kwaliteit van de identificatie. De PKI-infrastructuur biedt een keten van vertrouwen (chain of trust), de identiteiten zijn met een vastgestelde mate van betrouwbaarheid opgenomen in de certificaten. De organisatie die de identiteit vaststelt (TSP) ondertekent het certificaat met zijn certificaat. Als het certificaat niet is ingetrokken of verlopen is, dan kan men op de inhoud van het 'root' certificaat van de TSP vertrouwen.

De PKI-certificaten kunnen worden gebruikt bij de tweezijdige TLS-verbinding en voor de ondertekening en versleuteling van berichten zoals dit ook in Digikoppeling wordt toegepast. Op basis van het certificaat en dus ook de identiteit dat hierbij betrokken is kan de identiteit geauthenticeerd worden.

### Must: Gebruik Onderwijs Serviceregister

#### Endpoint

Het OSR functioneert als een soort van “gouden gids” waarin partijen de endpoints van services van verschillende dienstaanbieders kunnen opzoeken. In REST context hebben we het over resources, de resources moeten ook vindbaar zijn en worden in het OSR geregistreerd.

#### Profielaanduiding

Momenteel kunnen (Edukoppeling WUS) services geregistreerd worden in het Onderwijs Serviceregister. De OSR functies worden ook voor het REST/SaaS-profiel gebruikt. Er zullen mogelijk partijen zijn die de gegevens laten bewerken via een REST- en WUS-koppelvlak en kan een profielaanduiding in het OSR wenselijk zijn.

#### Mandatering

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.

De resources zullen afhankelijk van hun classificatie binnen de context van de mandatering moeten vallen.

## Specifieke voorschriften REST/SaaS-profiel

### Must: Routering o.b.v. (HTTP headerr/JWT)

Het Edukoppeling WUS profiel ondersteunt het kunnen routeren naar een eindorganisatie op basis van de WS-Addressing (WSA[[8]](#footnote-8)) 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](https://jwt.io/)

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.

### Should: Aansluiten op overheidsbrede afspraken rond REST

De basis van dit profiel wordt gevormd door de overheidsbrede afspraken die ontwikkelt zijn als onderdeel van de API-strategie[[9]](#footnote-9) en Design rules extensies[[10]](#footnote-10). De principes in deze documenten zijn nog niet formeel vastgesteld en nog in ontwikkeling, maar worden hieronder wel als voorschrift overgenomen. Indien we er in dit profiel op afwijkingen dan is dit expliciet aangegeven. Als we het volledig overnemen dan geldt een Must, alle andere kwalificaties betekenen dat we hier in bepaalde mate van afwijken.

#### REST 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[[11]](#footnote-11)
* 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[[12]](#footnote-12) 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[[13]](#footnote-13):

* 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[[14]](#footnote-14):

* W: API-11: Encrypt connections using at least TLS v1.3, voor dit profiel gelden de voorschriften van UBV[[15]](#footnote-15)
* W: API-12: Allow access to an API only if an API key is provided, voor dit profiel geldt dat een API-key niet gebruikt wordt[[16]](#footnote-16)
* C: API-13: Accept tokens as HTTP headers only
* C: API-14: OAuth 2.0 can be used for authorisation[[17]](#footnote-17)
* M: API-15: Use PKIoverheid certificates for API authentication (onderdeel van het UBV Mutual TLS PKIo profiel)[[18]](#footnote-18)
* W: API-49: Use public API-key's, , voor dit profiel geldt dat een API-key niet gebruikt wordt, zie ook API-12[[19]](#footnote-19)
* W: API-50:: Use CORS to control access[[20]](#footnote-20), voor dit profiel geldt dat CORS niet relevant is

#### 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 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

* W: API-43: Apply caching to improve performance, voor dit profiel geldt dat caching niet relevant is[[21]](#footnote-21)

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[[22]](#footnote-22)
* M: API-47: Use the required HTTP status codes

# Bijlage A: OAuth

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 / ander profiel. De verdere invulling wordt gedefinieerd door Auth profielen. Er is een Oauth web profiel dat door Forum Standaardisatie op ptolu-lijst gezet gaat worden.

De API-strategie stelt als principe “Use OAuth 2.0 for authorisation” (API-14). Als invulling hiervoor is er een OAuth profiel[[23]](#footnote-23) in ontwikkeling. Als functioneel toepassingsgebied wordt het volgende voorgesteld: “*Het gebruik van OAuth 2.0 is 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*”.

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.

# Bijlage B: Foutafhandeling (Authorisation errors)

1. <https://www.geonovum.nl/themas/kennisplatform-apis> [↑](#footnote-ref-1)
2. <https://www.edustandaard.nl/standaard_afspraken/open-onderwijs-api/open-onderwijs-api/> [↑](#footnote-ref-2)
3. <https://geonovum.github.io/KP-APIs/API-strategie-algemeen/> [↑](#footnote-ref-3)
4. https://www.edustandaard.nl/app/uploads/2019/02/2019-01-31-Edukoppeling-Architectuur-1.2.2-definitief.pdf [↑](#footnote-ref-4)
5. Meer informatie via Werkgroep Uniforme Beveiligingsvoorschriften: https://www.edustandaard.nl/standaard\_werkgroepen/uniforme-beveiligingsvoorschriften-in-oprichting/ [↑](#footnote-ref-5)
6. 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. [↑](#footnote-ref-6)
7. <https://www.owasp.org/index.php/OWASP_API_Security_Project> [↑](#footnote-ref-7)
8. <https://www.w3.org/TR/ws-addr-core/> [↑](#footnote-ref-8)
9. https://geonovum.github.io/KP-APIs/API-strategie-algemeen/ en https://geonovum.github.io/KP-APIs/API-strategie-extensies/ (15-07-2019) [↑](#footnote-ref-9)
10. De extensies zijn nog in ontwikkeling, zie <https://docs.geostandaarden.nl/api/API-Strategie-ext/> [↑](#footnote-ref-10)
11. De HTTP HEAD, TRACE, OPTIONS en CONNECT operations are in the context of REST hardly ever used and have been excluded [↑](#footnote-ref-11)
12. <https://github.com/OAI/OpenAPI-Specification> [↑](#footnote-ref-12)
13. Er zijn richtlijnen voor versioning in API strategie opgenomen, maar geen principes. [↑](#footnote-ref-13)
14. De API strategie kenmerkt dit onderdeel als niet normatief. [↑](#footnote-ref-14)
15. We wijken af van de API strategie. [↑](#footnote-ref-15)
16. We wijken af van de API strategie. [↑](#footnote-ref-16)
17. We wijken af van de API strategie, zie bijlage A [↑](#footnote-ref-17)
18. De API strategie beperkt de toepassing access-restricted or purpose-limited API’s [↑](#footnote-ref-18)
19. We wijken af van de API strategie [↑](#footnote-ref-19)
20. We wijken af van de API strategie, dit profiel gaat uit van communicatie tussen een client en server en er geldt geen verplichting. [↑](#footnote-ref-20)
21. We wijken af van de API strategie [↑](#footnote-ref-21)
22. <https://tools.ietf.org/html/rfc7807> [↑](#footnote-ref-22)
23. <https://geonovum.github.io/KP-APIs-OAuthNL/#dutch-government-assurance-profile-for-oauth-2-0> [↑](#footnote-ref-23)