Edukoppeling

***M2M gegevensuitwisseling binnen het onderwijs***

*Mandated Data eXchange (MDX) Secure API REST profile*

Edustandaard

Datum: maart 2023

Versie: 1.1

**Inhoudsopgave**

[1. Status van dit document 3](#_Toc131077011)

[1.1. Documenthistorie 3](#_Toc131077012)

[1.2. Overzicht actuele documentatie en compliance 3](#_Toc131077013)

[2. Inleiding 4](#_Toc131077014)

[2.1. Aanleiding voor het ontwikkelen van de Edukoppeling standaard 4](#_Toc131077015)

[2.2. MDX Secure API REST profile 4](#_Toc131077016)

[2.3. Doel en doelgroep 4](#_Toc131077017)

[2.4. Positionering binnen Edukoppeling Architectuur 5](#_Toc131077018)

[2.5. Functioneel toepassingsgebied 5](#_Toc131077019)

[2.6. Notatiewijze voorschriften 6](#_Toc131077020)

[2.7. Leeswijzer 6](#_Toc131077021)

[3. Voorschriften REST 7](#_Toc131077022)

[3.1. MUST: API Design conform het Digikoppeling REST profiel 7](#_Toc131077023)

[3.2. MUST: Routeringskenmerken zijn opgenomen als query parameters 9](#_Toc131077024)

[3.3. MAY: Berichtbeveiligingsvoorschriften 10](#_Toc131077025)

[3.4. MUST: Foutafhandeling m.b.t. het routeringskenmerk 10](#_Toc131077026)

[4. Overige voorschriften 11](#_Toc131077027)

[4.1. MAY: Gebruik van openbare internet 11](#_Toc131077028)

[4.2. MUST: Transportbeveiliging op basis van mTLS 11](#_Toc131077029)

[4.3. MUST: Identificatie en authenticatie van organisaties 11](#_Toc131077030)

[4.4. MAY: Kan worden toegepast voor zowel bevragingen als meldingen 12](#_Toc131077031)

[4.5. MUST: Toepassing van het MDX OSR protocol 13](#_Toc131077032)

[4.6. MUST: Foutafhandeling m.b.t. het routeringskenmerk 13](#_Toc131077033)

#

# Status van dit document

Dit document is een concept van de Edukoppeling MDX Secure API REST profile versie 1.1.

# Documenthistorie

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versie** | **Status** | **Auteur** | **Datum** | **Opmerking** |
| 1.0 | Vastgesteld | Werkgroep Edukoppeling | februari 2021 | Zie release notes |
| 1.1 | Concept | Werkgroep Edukoppeling | maart 2023 | De impact van deze 1.1 is beperkt en betreft met name tekstuele wijzigingen. Wel zijn een aantal API Design Rules gewijzigd.* De naam is gewijzigd van “Edukoppeling - REST\_SaaS-profiel” naar “MDX Secure API REST profile“
* Tekst (begrippen) ivm herziening ROSA (issue #50)
* Foutmelding Mandatering (issue #49)
* Figuur 1 aangepast ivm REST-profiel versie 1.1, UBV TLS en OAuth-profiel
* Aansluiting op Digikoppeling REST profiel. In deze conceptversie is een kopie van de ADR principes opgenomen voor leesbaarheid (willen we dit of ref naar document DK opnemen?).
* Aangepast: Er is in de tussentijd een nieuwe ADR versie gekomen waar Digikoppeling REST gebruik van maakt. Een aantal normatieve principes zijn iets anders verwoord of zijn vervallen. In tabel (die ook in het OAuth profiel is opgenomen worden wijzigingen tov versie 1.0 aangegeven)
 |

# Overzicht actuele documentatie en compliance

Dit document (MDX Secure API REST profile) staat niet op zichzelf (zie Figuur 1). Het document “Overzicht actuele documentatie en compliance juni 2023” geeft een actueel overzicht van de verschillende normatieve en informatieve Edukoppeling documenten.

# Inleiding

# Aanleiding voor het ontwikkelen van de Edukoppeling standaard

De aanleiding voor de introductie van Edukoppeling in het onderwijsdomein is een steeds groter wordende stroom van geautomatiseerde machine-machine uitwisselingen in het onderwijs. Dit wordt veroorzaakt door vernieuwingen in het onderwijs zelf, in wetgeving en in de beschikbare techniek. In toenemende mate lopen de processen over organisaties heen, tussen onderwijsorganisaties (zowel op bestuursniveau van de onderwijsaanbieders, de “scholen”) onderling, tussen onderwijsorganisaties en overheidsorganisaties en tussen onderwijsorganisaties en private onderwijsgerelateerde organisaties. En vaak, als er iets nieuws komt, wordt er dan pas nagedacht over de benodigde wijze van koppelen. Als men niet oppast worden er evenveel verschillende soorten van koppelingen bedacht als er geautomatiseerde processen zijn. Dat is nadelig, omdat hiervoor veel kennis nodig is, dit onnodig veel en kostbaar onderhoudt vergt, dit de interoperabiliteit en aanpasbaarheid hindert. Met Edukoppeling verandert dat. Edukoppeling is een meervoudig inzetbare wijze van koppelen waarvan de ontwikkeling en het beheer gemeenschappelijk wordt aangepakt. Edukoppeling is tevens een open standaard, wat maakt dat partijen met een lage drempel kunnen deelnemen, wat gunstig is voor het onderwijs.

In het onderwijs is het normaal geworden dat onderwijsinstellingen veel van hun processen laten ondersteunen door zogeheten SaaS-diensten (diensten ‘in the cloud’)*.* Dit geldt voor onderwijskundige processen als ook voor hun administratieve processen. Het Edukoppeling Mandated Data eXchange[[1]](#footnote-1) (MDX) protocol en verwante profielen houden met deze ontwikkeling rekening. De diensten van leveranciers waar een onderwijsorganisatie gebruik van maakt beheren gegevens (administraties) en wisselen vaak namens de onderwijsorganisatie gegevens uit met ketenpartijen. De Edukoppeling Mandated Data eXchange profielen houden expliciet rekening met het uitwisselen van gegevens tussen verwerkers (bijvoorbeeld leveranciers) namens een eindorganisatie (bijvoorbeeld een onderwijsorganisatie).

# MDX Secure API REST profile

Dit document beschrijft het Edukoppeling MDX Secure API REST profile (verder aangeduid als REST-profiel) en is onderdeel van de Edukoppeling Architectuur. Bij dit REST-profiel is het Mandated Data eXchange (MDX) protocol, mTLS/PKIo en het gebruik van het routeringskenmerk van toepassing. Er wordt van een synchrone point-to-point koppeling uitgegaan en het routeringskenmerk in de respons is de inverse van het request[[2]](#footnote-2). Binnen de scope van dit profiel wordt toegang tot een protected resource gegeven op basis van mTLS authenticatie en het OIN in het client certificaat.

# Doel en doelgroep

Het doel dat met dit profiel nagestreefd wordt is het op een generieke manier kunnen uitwisselen van gegevens binnen de onderwijssector. Het profiel ondersteunt zowel het scenario waarbij een Eindorganisatie zijn systeem zelf beheert in de eigen ICT-infrastructuur, als het scenario waarbij de Eindorganisatie deze als (SaaS-)dienst van een verwerker (leverancier) afneemt.

Dit document is bedoeld voor ICT-specialisten die betrokken zijn bij het ontwerpen en ontwikkelen van systeem-naar-systeem (M2M) koppelingen. Het gaat hier om werknemers (ontwikkelaars, architecten, projectmanagers, informatiemanagers etc.) werkzaam bij onderwijsgerelateerde organisaties, zowel in de publieke als private sector. Edukoppeling is voor een groot deel compliant aan de overheidsstandaard Digikoppeling. De Edukoppeling-documentatie dient derhalve naast de Digikoppeling-documentatie gebruikt te worden.

De lezer van dit document willen wij vragen om zaken die ontbreken of onduidelijk zijn te melden bij de beheerorganisatie Edustandaard[[3]](#footnote-3).

# Positionering binnen Edukoppeling Architectuur

Het Edukoppeling REST-profiel is onderdeel van de Edukoppeling Architectuur. Het vereist naast de toepassing van het MDX OSR protocol een aantal API Design Rules. Deze Design Rules zijn overgenomen van de Digikoppeling Koppelvlakstandaard REST-API 1.1.1[[4]](#footnote-4).



Figuur - Positionering van REST-profiel binnen de Edukoppeling Architectuur

# Functioneel toepassingsgebied

Het functionele toepassingsgebied van dit REST-profiel betreft M2M-gegevensuitwisseling via een point-to-point verbinding voor uitwisseling van vertrouwelijke gegevens via een gesloten API[[5]](#footnote-5). Er worden bevragingen (pull) en meldingen (push) op basis van een request-response uitwisselingspatroon ondersteund. De systemen die de uitwisseling uitvoeren worden beheerd door verwerkers[[6]](#footnote-6) en doen dit op basis van een mandaat van een eindorganisatie (het MDX OSR protocol is van toepassing). De verwerker kan de gegevens verder routeren naar een eindorganisatie op basis van het routeringskenmerk. Het profiel kan ook worden toegepast indien de eindorganisatie ook zelf de rol van verwerker heeft.

# Notatiewijze voorschriften

Voor elk voorschrift wordt aangegeven in welke mate hier invulling aan moet worden gegeven. Hiermee kunnen we duidelijk aangeven wat de grenzen van dit profiel zijn ten opzichte van de mogelijke externe bron(nen) waar het voorschrift eventueel van wordt overgenomen. We gebruiken hiervoor de notatiewijze van RFC2119[[7]](#footnote-7). Deze gebruikt de volgende termen: "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL".

# Leeswijzer

[todo]

# Voorschriften REST

Voor het Edukoppeling REST-profiel wordt zoveel mogelijk aangesloten op de nationale Digikoppeling standaard, Dit REST-profiel neemt derhalve een aantal voorschriften over van de Digikoppeling Koppelvlakstandaard REST-API. Er worden ook een aantal afwijkende voorschriften geformuleerd. De specifieke REST voorschriften zijn:

1. Het Edukoppeling REST-profiel stelt eisen aan API Design (protected resource).
2. Het Edukoppeling REST-profiel eist dat de routeringskenmerken zijn opgenomen als query parameters in het request naar het token endpoint van de Authorization Server.

### MUST: API Design conform het Digikoppeling REST profiel

API design moet conform de API Design Rules zijn van het Digikoppeling Restful API profiel[[8]](#footnote-8).

De API Design principes zijn ook een belangrijk onderdeel van het Edukoppeling MDX Secure API REST profiel versie 1.0 (hierna REST-profiel). De API Design principes zijn echter sinds publicatie van de 1.0 versie van het REST-profiel gewijzigd. Hieronder wordt aangegeven welke principes voor het huidige REST-profiel versie 1.0 gelden en welke voor deze nieuwe versie van het REST-profiel[[9]](#footnote-9) gelden. Bij gewijzigde principes is het nummer rood gekleurd, bij nieuwe groen en bij ongewijzigd zwart. De principes met een grijze achtergrond vulling zijn de API extensies[[10]](#footnote-10). Vanuit het Digikoppeling Koppelvlakstandaard REST-API worden er per principe een kwalificatie toegekend. Deze zijn in de tabel hieronder overgenomen.

|  |  |  |
| --- | --- | --- |
| **#** | **MDX Secure API REST profile v1.0** | **MDX Secure API REST profile v1.1** |
| API-01 | Operations are Safe and/or Idempotent | Verplicht: [Adhere to HTTP safety and idempotency semantics for operations](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-01) |
| API02 | Do not maintain state at the server | Verplicht: [Do not maintain session state on the server](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-02) |
| API03 | Only apply default HTTP operations | Verplicht: [Only apply standard HTTP methods](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-03) |
| API04 | Define interfaces in Dutch unless there is an official English glossary available | Verplicht: [Define interfaces in Dutch unless there is an official English glossary available](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-04) |
| API05 | Use plural nouns to indicate resources | Verplicht: [Use nouns to name resources](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-05) |
| API-06 | Create relations of nested resources within the endpoint | Verplicht: [Use nested URIs for child resources](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-06) |
| API-09 | Implement custom representation if supported | *Vervallen* |
| API-10 | Implement operations that do not fit the CRUD model as sub-resources | Verplicht: [Model resource operations as a sub-resource or dedicated resource](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-10) |
| API-11 | Encrypt connections using TLS following the latest NCSC guidelines | *Niet van toepassing, TLS voorschriften zijn opgenomen in UBV TLS.* |
| API-12 | Allow access to an API only if an API key is provided | *Vervallen* |
| API-13 | Accept tokens as HTTP headers only | Verplicht: [Accept tokens as HTTP headers only](https://docs.geostandaarden.nl/api/def-hr-API-Strategie-ext-20211013/#api-13)  |
| API-14 | OAuth 2.0 can be used for authorisation | *Vervallen* |
| API-15 | Use PKIoverheid certificates for access-restricted or purpose-limited API authentication | *Vervallen* |
| API-16 | Documentation conforms to OAS v3.0 or newer | Verplicht: [Use OpenAPI Specification for documentation](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-16) |
| API-17 | Publish documentation in Dutch unless there is existing documentation in English or there is an official English glossary available | Verplicht: [Publish documentation in Dutch unless there is existing documentation in English](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-17) |
| API-18 | Include a deprecation schedule when publishing API changes | Verplicht: [Include a deprecation schedule when publishing API changes](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-18) |
| API-19 | Allow for a (maximum) 1 year transition period to a new API version | Verplicht: [Schedule a fixed transition period for a new major API version](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-19) |
| API-20 | Include the major version number only in ihe URI | Verplicht: [Include the major version number in the URI](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-20) |
| API-21 | Inform users of a deprecated API actively | *Vervallen* |
| API-22 | JSON first - APIs receive and send JSON | *Vervallen* |
| API-23 | APIs may provide a JSON Schema | *Vervallen* |
| API-24 | Support content negotiation | *Vervallen* |
| API-25 | Check the Content-Type header settings | *Vervallen* |
| API-26 | Define field names in camelCase | *Vervallen* |
| API-27 | Disable pretty print | *Vervallen* |
| API-28 | Send a JSON-response without enclosing envelope | *Vervallen* |
| API-29 | Support JSON-encoded POST, PUT, and PATCH payloads | *Vervallen* |
| API-30 | Use query parameters corresponding to the queryable fields | *Vervallen* |
| API-31 | Use the query parameter sorteer to sort | *Vervallen* |
| API-32 | Use the query parameter zoek for full-text search | *Vervallen* |
| API-33 | Support both \* and ? wildcard characters for full-text search APIs | *Vervallen* |
| API-34 | Support GeoJSON for GEO APIs | *Vervallen* |
| API-35 | Include GeoJSON as part of the embedded resource in the JSON response | *Vervallen* |
| API-36 | Provide a POST endpoint for GEO queries | *Vervallen* |
| API-37 | Support mixed queries at POST endpoints | *Vervallen* |
| API-38 | Put results of a global spatial query in the relevant geometric context | *Vervallen* |
| API-39 | Use ETRS89 as the preferred coordinate reference system (CRS) | *Vervallen* |
| API-40 | Pass the coordinate reference system (CRS) of the request and the response in the headers | *Vervallen* |
| API-41 | Use content negotiation to serve different CRSs | *Vervallen* |
| API-42 | Use JSON+HAL with media type application/hal+json for pagination | *Vervallen* |
| API-43 | Apply caching to improve performance | *Vervallen* |
| API-44 | Apply rate limiting | *Vervallen* |
| API-45 | Provide rate limiting information | *Vervallen* |
| API-46 | Use default error handling | *Aanbevolen*: [Use default error handling](https://docs.geostandaarden.nl/api/def-hr-API-Strategie-ext-20211013#api-46)  |
| API-47 | Use the required HTTP status codes | *Aanbevolen*: [Use the required HTTP status codes](https://docs.geostandaarden.nl/api/def-hr-API-Strategie-ext-20211013#api-47) |
| API-48 | Leave off trailing slashes from API endpoints | [Leave off trailing slashes from URIs](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-48) |
| API-49 | Use public API-keys | *Vervallen* |
| API-50 | Use CORS to control access | *Vervallen* |
| API-51 | Publish OAS at a base-URI in JSON-format | Verplicht: [Publish OAS document at a standard location in JSON-format](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-51) |
| API-52 | Use OAuth 2.0 for authorisation with rights delegation | *Vervallen* |
| API-53 | - | Verplicht: [Hide irrelevant implementation details](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-53) |
| API-54 | - | Verplicht: [Use plural nouns to name collection resources](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-54) |
| API-55 | - | Verplicht: [Publish a changelog for API changes between versions](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-55) |
| API-56 | - | Verplicht: [Adhere to the Semantic Versioning model when releasing API changes](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-56) |
| API-57 | - | Verplicht: [Return the full version number in a response header](https://publicatie.centrumvoorstandaarden.nl/api/adr/#api-57) |
| API-58 | - | Verplicht: [No sensitive information in URIs](https://docs.geostandaarden.nl/api/def-hr-API-Strategie-ext-20211013/#api-58)  |

Over het algemeen zijn de wijzigingen enkel van tekstuele aard. De nieuwe principes hebben wel impact.

### MUST: Routeringskenmerken zijn opgenomen als query parameters

Een belangrijk aspect van MDX-profielen is het kunnen routeren naar een eindorganisatie. Bij de point-to-point (TLS) verbinding tussen de verwerker rollen moet er gerouteerd kunnen worden naar de eindorganisatie. De eindorganisaties worden middels een FROM en een TO routeringskenmerk gespecificeerd. Het kan zijn dat partijen gegevens uitwisselen voor de zelfde eindorganisatie. Ook al zijn dat de FROM en TO routeringskenmerk hetzelfde deze worden altijd gevuld.

In dit REST-profiel (en het MDX Secure API OAuth profile) worden de FROM (edu-from) en TO (edu-to) routeringskenmerken als query parameters opgenomen als onderdeel van het request. Hierdoor is het voor de ontvanger direct duidelijk vanuit welke eindorganisatie het bericht verstuurd is, en voor welke het bedoeld is. Gezien het een synchrone point-to-point koppeling betreft (een bilaterale koppeling zonder intermediairs) wordt impliciet gesteld dat de edu-from parameter in het request de edu-to parameter in de response is en de edu-to parameter in het request de edu-from parameter in de response is. We ondersteunen dus de use case waar zowel client als server een verwerker zijn en er aan beide kanten naar dezelfde (of verschillende) eindorganisatie gerouteerd kan worden.

Een voorbeeld wordt hieronder weergegeven. Hierin communiceren twee partijen als verwerker gegevens naar dezelfde eindorganisatie:

<https://prod.leverancier.com/v1/service?edu-to=0000000700011BB00001&edu-from=0000000700011BB00000>

Het routeringskenmerk wordt geleverd bij het request van elke HTTP methode. Mede op basis van het routeringskenmerk (zie MDX OSR protocol) kan de mandatering gevalideerd worden. Als één of beide routeringskenmerken in het request ontbreken moet er een foutmelding (zie MUST: Foutafhandeling m.b.t. het routeringskenmerk) gegeven worden.

### MAY: Berichtbeveiligingsvoorschriften

Berichtbeveiliging naast transportbeveiliging is met name relevant in ketens met transparante intermediairs. Het ondertekenen van het bericht kan wenselijk zijn om onweerlegbaarheid[[11]](#footnote-11) te ondersteunen.

Voor dit REST-profiel zijn momenteel geen berichtbeveiligingsvoorschriften opgenomen en heeft hiermee in vergelijking tot het MDX Secure API WUS-profiel beperkte functionaliteit. Wel zijn er ontwikkelingen rond berichtbeveiliging voor RESTful uitwisselingen (zie Digikopppeling REST profiel[[12]](#footnote-12))

### MUST: Foutafhandeling m.b.t. het routeringskenmerk

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Status code** | **Omschrijving** | **Categorie** | **Domein** | **Toelichting** |
| 400 | Bad Request | Syntax | EK | To routeringskenmerk ontbreekt |
| 400 | Bad Request | Syntax | EK | To routeringskenmerk is geen OIN |
| 400 | Bad Request | Syntax | EK | From routeringskenmerk ontbreekt |
| 400 | Bad Request | Syntax | EK | From routeringskenmerk is geen OIN |
| 403 | Forbidden |  Mandatering | EK  |  Autorisatiefout* TLS: OIN in certificaat niet geautoriseerd
* TLS: OIN in certificaat niet gemandateerd om voor eindorganisatie (From routeringskenmerk) in context van deze API gegevens uit te wisselen
 |
| 404 | Not Found |   |   | De server kan resource niet vinden. Het endpoint kan echter valide zijn. Een server kan deze code sturen ipv code 403 om het eventuele bestaan van de resources niet vrij te geven aan een niet geautoriseerde client |

# Overige voorschriften

Er zijn verschillende MDX profielen (WUS, REST en OAuth) waarvoor een aantal generieke voorschriften gelden. Deze generieke voorschriften worden in dit hoofdstuk beschreven. Het betreft het volgende:

1. Het Edukoppeling REST-profiel houdt expliciet rekening met gebruik van een openbaar netwerk (Internet).
2. Het Edukoppeling REST-profiel stelt eisen aan transportbeveiliging.
3. Het Edukoppeling REST-profiel stelt eisen aan identificatie en authenticatie van organisaties.
4. Het Edukoppeling REST-profiel kan worden toegepast voor zowel bevragingen als meldingen
5. Het Edukoppeling REST-profiel wordt in combinatie met het MDX OSR protocol gebruikt.
6. Het Edukoppeling REST-profiel stelt eisen aan foutafhandeling m.b.t. het routeringskenmerk.

### MAY: 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: Transportbeveiliging op basis van mTLS[[13]](#footnote-13)

De MDX profielen maken voor transportbeveiliging gebruik van mTLS. De voorschriften hiervoor zijn opgenomen in de Edustandaard Uniforme Beveiligingsvoorschriften (UBV TLS Edukoppeling profiel[[14]](#footnote-14)).

Er wordt verder aanbevolen om bedreigingen rond beschikbaarheid, integriteit en vertrouwelijkheid te beperken door het opvolgen van OWASP-richtlijnen[[15]](#footnote-15).

### MUST: Identificatie en authenticatie van organisaties

Identificatie

Binnen ketens waarbij een Edukoppeling MDX profiel wordt toegepast voor de gegevensuitwisseling, worden partijen geïdentificeerd op basis van hun unieke Organisatie Identificatie Nummer (OIN)[[16]](#footnote-16). Onderwijsorganisaties worden geïdentificeerd op basis van het BRIN. Binnen de OIN-systematiek betekent dit dat het OIN hoofdnummer een BRIN is en een prefix met de waarde “00000007”. Voor bedrijven wordt een systematiek gebruikt die gelijk is aan de OIN-systematiek en wordt ook wel HRN genoemd. Voor het HRN wordt alleen de prefix 00000001 (RSIN als hoofdnummer) of 00000003 (KvK nummer als hoofdnummer) gebruikt.

In de Edukoppeling Architectuur worden binnen de MDX profielen drie[[17]](#footnote-17) rollen onderscheiden, dit REST-profiel gaat uit van de volgende twee rollen:

1. De Eindorganisatie is de organisatie die in het kader van zijn doelstellingen samenwerkt met een andere organisatie.
2. De Verwerker is een organisatie die in opdracht van de eindorganisatie vertrouwelijke gegevens verwerkt[[18]](#footnote-18).

De eindorganisatie binnen een Edukoppeling MDX profiel betreft vaak een onderwijsorganisatie, maar kan ook een bedrijf of ZBO betreffen. Binnen de gegevensuitwisseling wordt het OIN van de eindorganisatie opgenomen in het zogenaamde ‘TO’ en ‘FROM’ routeringskenmerken.

De verwerker binnen een Edukoppeling MDX profiel betreft vaak een bedrijf, maar kan ook een onderwijsorganisatie of een ZBO betreffen. Binnen de gegevensuitwisseling is het OIN (HRN) van de verwerker in het PKIoverheid-certificaat opgenomen dat wordt gebruikt bij de mTLS-verbinding.

Authenticatie verwerker

Binnen de Edukoppeling MDX profielen worden beide verwerkers geauthenticeerd door toepassing van een PKI-infrastructuur. De PKI-infrastructuur (PKIo) 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 (Trust Service Providers) ondertekent het certificaat van de verwerker met zijn (CA) certificaat. Het certificaat van een verwerker wordt gebruikt in de mTLS verbinding. De voorschriften rond mTLS zijn opgenomen in de Edustandaard UBV TLS standaard[[19]](#footnote-19).

Authenticatie verwerkers op basis van mTLS (bij Authorization Server Token Endpoint)

De MDX-profielen vereisen dat verwerkers elkaar kunnen authenticeren op basis van mTLS. Dit wordt toegepast conform het Edukoppeling profiel in de UBV TLS voorschriften. Het Edukoppeling profiel binnen de UBV TLS afspraak maakt deels gebruik van de Digikoppeling beveiligingsvoorschriften, zoals het gebruik van PKIoverheid certificaten (UBV-TLS-PKI-01/ DK-TLS001[[20]](#footnote-20)) en de toepassing van mTLS (DK-TLS002). De certificaten worden uitgegeven door erkende Trust Service Providers (TSP’s). Hierbij wordt het OIN/HRN vastgesteld door de TSP, op basis van het door de aanvrager opgegeven KvK-nummer, dat door de TSP wordt gecontroleerd. De PKI-overheidscertificaten zijn van het niveau STORK QAA 4[[21]](#footnote-21). Bij de uitgifte hoort ‘face-to-face’ controle: de houder neemt het certificaat persoonlijk in ontvangst. Het identificerend kenmerk wordt conform Digikoppeling OIN nummersystematiek bepaalt (zie identificatie en authenticatie[[22]](#footnote-22)). De TSP die het certificaat uitgeeft heeft de verantwoordelijkheid om de uniciteit van het subject te waarborgen en de identiteit te vermelden in het certificaat in het veld Subject.serialNumber.

### MAY: Kan worden toegepast voor zowel bevragingen als meldingen

De Edukoppeling MDX profielen ondersteunt standaard de synchrone bevraging (pull) en synchrone melding (push) transactiepatronen. Andere transactiepatronen kunnen echter ook worden ondersteund (zie Edukoppeling Architectuur).

Dit sluit ook aan bij de (actuele[[23]](#footnote-23)) versie van de Digikoppeling architectuur en de Digikoppeling WUS en REST profielen. In vorige versies van de Digikoppeling Architectuur werden specifieke profielen gekoppeld aan bevragingen (WUS/REST) en meldingen (ebMS). Dit voorschrift bleek in de praktijk niet meer goed bruikbaar. Vandaar dat met ingang van versie 2.0.0 deze relatie is komen te vervallen.

### MUST: Toepassing van het MDX OSR protocol

Onderwijsorganisaties maken in de context van MDX profielen gebruik van (SaaS) diensten van een leverancier. Het Onderwijs Service Register (OSR) onderkent deze situatie en ondersteunt tevens de functie om mandateringen te registreren en verifiëren. Het mandaat is de registratie dat een bepaalde verwerker (bijvoorbeeld SaaS-leverancier) namens een bepaalde eindorganisatie (bijvoorbeeld onderwijsorganisatie) door middel van een dienst via één of meer interfaces gegevens mag uitwisselen binnen een ketensamenwerking. Welke eisen er gelden rond het OSR zijn vastgelegd in het MDX OSR protocol.

### MUST: Foutafhandeling m.b.t. het routeringskenmerk

Edukoppeling definieert een aantal categorieën voor foutmeldingen. Deze zijn opgenomen in architectuur. De hier opgenomen foutmeldingen hebben betrekking op de eindorganisatie routeringskenmerken. Hoe deze gecommuniceerd worden zijn uniek per MDX profiel. Voor dit REST-profiel zijn deze gelijk aan die van het MDX Secure API OAuth profile.

|  |  |  |
| --- | --- | --- |
| **Omschrijving** | **Categorie** | **Toelichting** |
| To parameter ontbreekt | A (Syntax) | Ontvanger niet ingevuld |
| To parameter is geen OIN | A (Syntax) | Ontvanger parameter is geen valide OIN  |
| From parameter ontbreekt | A (Syntax) | Afzender niet ingevuld |
| From parameter is geen OIN | A (Syntax) | Afzender parameter is geen valide OIN  |

1. Voorheen werden de betreffende profielen ook wel SaaS-profielen genoemd. Omdat hier vaak discussie bij ontstond omdat het niet altijd een SaaS-dienst /SaaS-leverancier betrof is de nieuwe naam Mandated Data eXchange geïntroduceerd vanaf deze versie. Dit geldt ook voor alle andere stukken die na maart 2023 zijn gepubliceerd [↑](#footnote-ref-1)
2. De edu-from parameter van het request is de edu-to parameter in de response, de edu-to parameter in het request is de edu-from parameter in de response. [↑](#footnote-ref-2)
3. <https://www.edustandaard.nl/standaarden/afspraken/afspraak/edukoppeling/>. Reageren kan via info@edustandaard.nl. [↑](#footnote-ref-3)
4. [Digikoppeling Koppelvlakstandaard REST-API 1.1.1 (centrumvoorstandaarden.nl)](https://publicatie.centrumvoorstandaarden.nl/dk/restapi/) [↑](#footnote-ref-4)
5. Het Kennisplatform API’s heeft o.a. een API Strategie ontwikkeld waarin verschillende soorten API's worden onderkend (<https://geonovum.github.io/KP-APIs/API-strategie-algemeen/>). Open API's: *voor ontsluiten van diensten zonder toegangsbeperking bijv. open data*. Gesloten API's: *voor ontsluiten van diensten met toegangsbeperking bijv. persoonsgegevens en vertrouwelijke gegevens of diensten voor specifieke partijen (access-restricted and purpose-limited API’s)*. [↑](#footnote-ref-5)
6. Zie Edukoppeling Architectuur voor toelichting rond rollen binnen een MDX uitwisseling. [↑](#footnote-ref-6)
7. https://tools.ietf.org/html/rfc2119

 [↑](#footnote-ref-7)
8. <https://publicatie.centrumvoorstandaarden.nl/dk/restapi/#api-design-rules> [↑](#footnote-ref-8)
9. Hetzelfde geld voor het MDX Secure API OAuth profiel [↑](#footnote-ref-9)
10. <https://publicatie.centrumvoorstandaarden.nl/dk/restapi/#afspraken-api-design-rules-extensies> [↑](#footnote-ref-10)
11. Onweerlegbaarheid in de zin van: de verzender van de request/response kan niet ontkennen het bericht verzonden te hebben wanneer deze voorzien is van de digitale handtekening van de afzender. Zie Digikoppeling REST profiel [↑](#footnote-ref-11)
12. <https://publicatie.centrumvoorstandaarden.nl/dk/restapi/#bijlage-gebruik-van-signing-encryptie-in-de-context-van-http-rest-api> [↑](#footnote-ref-12)
13. Het OAuth-profiel wijkt af van de andere MDX profielen doordat bij het koppelvlak met de Resource Server TLS wordt gebruikt. [↑](#footnote-ref-13)
14. Meer informatie via Werkgroep Uniforme Beveiligingsvoorschriften: <https://www.edustandaard.nl/standaard_afspraken/uniforme-beveiligingsvoorschriften/> [↑](#footnote-ref-14)
15. <https://www.owasp.org/index.php/OWASP_API_Security_Project> [↑](#footnote-ref-15)
16. Zie voor details de OIN nummersystematiek in het Edukoppeling Identificatie en Authenticatie document. [↑](#footnote-ref-16)
17. We gaan in dit REST-profiel uit van een point-to-point verbinding tussen de verwerkers (geen logistieke dienstverlener). [↑](#footnote-ref-17)
18. Verzamelt, opslaat, berekeningen uitvoert, verstrekt en dergelijke. [↑](#footnote-ref-18)
19. <https://www.edustandaard.nl/standaard_afspraken/uniforme-beveiligingsvoorschriften/> [↑](#footnote-ref-19)
20. <https://www.edustandaard.nl/standaard_afspraken/uniforme-beveiligingsvoorschriften/> [↑](#footnote-ref-20)
21. <https://www.cs.ru.nl/E.Verheul/SIO2019/D2.3_final.pdf> [↑](#footnote-ref-21)
22. <https://www.logius.nl/diensten/digikoppeling/documentatie> [↑](#footnote-ref-22)
23. <https://publicatie.centrumvoorstandaarden.nl/dk/architectuur/> [↑](#footnote-ref-23)