Programma van Eisen

Elektronische gegevensuitwisseling

tussen onderwijs organisaties en de Dienst Uitvoering Onderwijs

met betrekking tot het Register Instellingen en Opleidingen (RIO)

Versie: 0.9 Final draft Datum: 29-05-2019

Versiebeheer

Versie	Reden van versie	Auteurs	Datum
0.01	Nieuw Initiele opzet	G. de Koff	11-01-2018
0.1	Opmerkingen conf call met softwareleveranciers verwerkt	G. de Koff	19-01-2018
0.2	Doorstart na uitgestelde livegang, aangepast nav overleg en voortschrijdend inzicht	G. de Koff	04-09-2018
0.3	Wijzigingen in wijze terugkoppeling fouten Nieuw toegevoegde service om gewijzigde objecten op te vragen Alle services uitgewerkt nav besproken voorbeeldservice	G. de Koff	02-10-2018
0.4	Paragrafen over beveiliging en controles uitgewerkt	G. de Koff	01-11-2018
0.5	Kleine tekstuele aanpassingen H5 toelichting op RIO webservices uitgebreider beschreven Controles verplaatst naar los document ivm stabiliteit PvE	G. de Koff	27-11-2018
0.6	Review commentaar verwerkt	G. de Koff	12-04-2019
0.9	Webservice functionele werking tekstueel verduidelijkt	G. de Koff	27-05-2019

Inhoudsopgave

1. Inleiding

1.1. Algemeen

Dit document beschrijft de uitwisseling van RIO gegevens tussen onderwijs organisaties en DUO.
Het betreft het raadplegen van alle openbare onderdelen van RIO en het beheren van de eigen gegevens van de betreffende onderwijsorganisatie.

1.2. Leeswijzer

Dit programma van eisen beschrijft de uitwisseling tussen onderwijsorganisaties en de Dienst Uitvoering Onderwijs met betrekking tot het Register Instellingen en Opleidingen. De uitwisseling heeft op dit moment alleen betrekking op het VO en het MBO, maar zal in volgende versies worden uitgebreid met gegevens uit de sectoren PO en HO.

In dit document staan alle functionele afspraken en technische vereisten. De detailinformatie van de services zijn net als de XSD en de WSDL opgenomen in aparte bijbehorende documenten, zie hiervoor ook de volgende paragraaf.

1.3. Bijbehorende documenten

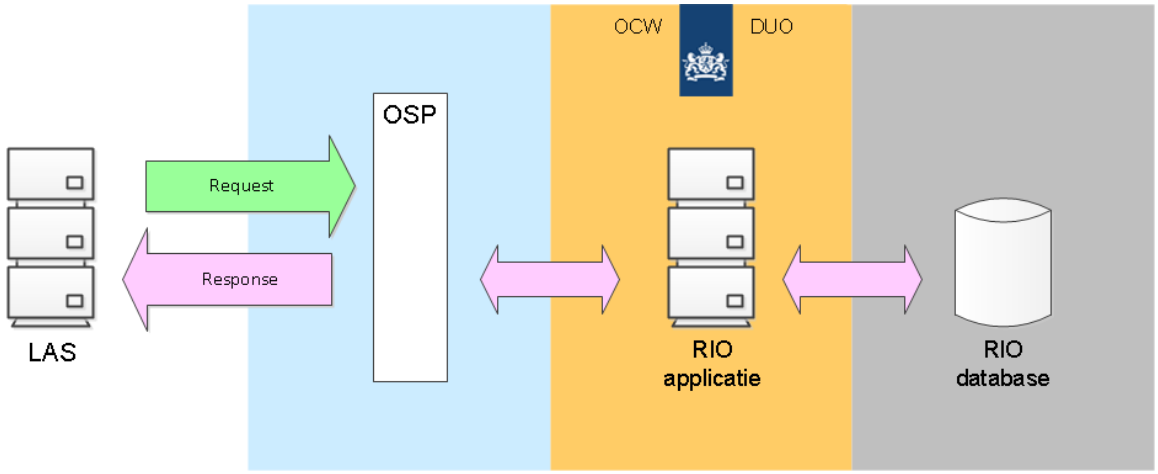
Naam	Versie
Webservice documentatie - DUO_RIO_Beheren_Raadplegen_OnderwijsOrganisatie_V1.docx	
DUO_RIO_Beheren_Raadplegen_OnderwijsOrganisatie_V1.wsdl	V1
DUO_RIO_Beheren_Raadplegen_OnderwijsOrganisatie_V1.xsd	V1
Webservice controles - DUO_RIO_Beheren_Raadplegen_OnderwijsOrganisatie_V1.docx	

2. Ontwerpkeuzes

2.1. Synchrone afhandeling (ipv asynchroon)

Het ontwerp van de webservices is gebaseerd op synchrone afhandeling van service-calls. Dit is zo gedaan vanuit het streven het eenvoudig te houden.

Hieronder een schema om synchrone verwerking te verduidelijken:



FIGUUR 1, SYNCHRONE AFHANDELING VAN BERICHTENVERKEER

2.2. Standen of mutaties

De bijgevoegde ontwerpen gaan uit van het leveren van standen. Alles wat voor de meegegeven set sleutelgegevens geleverd wordt in een bericht zal de bestaande stand in RIO overschrijven.

Aanvullende werkwijze aangegeven vanuit het overleg met de softwareleveranciers is om wel expliciet aan te geven als een registratie verwijderd moet worden. Dit om er voor te zorgen dat registraties niet onbedoeld verwijderd worden als ze per ongeluk niet meegeleverd worden in de stand.

2.3. Omvang van de berichten

Bij deze keuze voor synchroon uitwisselen in combinatie met standenleveringen moet de omvang van de stand zo gekozen worden dat het niet zo groot wordt dat er time-out problemen op gaan treden.

2.4. Technische standaarden

Qua technische standaarden (zie H6) is in dit PvE volledig aangesloten op de afspraken die in het project doorontwikkelen Bron-VO zijn gemaakt. Dit om er mede voor te zorgen dat vanuit de verschillende onderdelen van DUO hetzelfde koppelvlak geboden wordt aan partijen die met meerdere onderdelen van DUO uitwisselen.

Dit is zo op basis van de architectuur richtlijnen binnen DUO en mede op expliciet verzoek van enkele softwareleveranciers die al actief zijn in het VO veld en het MBO veld.

2.5. Foutcodes en teksten per attribuut

Het response bericht met eventuele foutmeldingen zal worden opgebouwd conform de opzet die al in gebruik is bij Bron.

2.6. RIO-schermen naast machine-machine verkeer

Op Duo.nl worden schermen aangeboden waarmee een onderwijsorganisatie de registraties in RIO kan beheren. Deze bestaan naast de in dit document beschreven machine-machine koppeling. Er wordt niet afgedwongen dat een onderwijsorganisatie uitsluitend het ene of het andere kanaal kan gebruiken. Hierdoor moet men binnen de onderwijsorganisatie zelf borgen dat de registraties synchroon blijven lopen.

2.7. Wijzigen van gegevens

Onderwijsinstellingen zijn zelf verantwoordelijk voor het correct vullen van RIO. Er zijn daarom in RIO ~~geen~~ alleen beperkingen op gebied van integriteit wat wel en wat niet gewijzigd mag worden aan de eigen gegevens (onderwijsaanbieder, onderwijslocatiegebruik, aangeboden opleidingen).

3. Definities

Dit hoofdstuk definieert alle relevante begrippen uit het Programma van Eisen.

Term/afkorting	Omschrijving
BRIN	Unieke code waarmee een onderwijsinstelling kan worden geïdentificeerd
BRON	Basis Register ONderwijs Het centrale register van inschrijvingen en resultaten voor de onderwijssectoren Voortgezet Onderwijs en Beroeps en Volwassenen Educatie
Digikoppeling	Digikoppeling is een set standaarden voor elektronisch berichtenverkeer tussen overheidsorganisaties. Vroeger heette het OverheidsService Bus. Het is een bouwsteen uit de NORA, digikoppeling is de 'postbode' voor de overheid.
Digimelding	Digimelding is één centraal punt voor het melden van onjuistheden in basisregistraties. Het melden gebeurt via Digikoppeling.
DUO	Dienst Uitvoering Onderwijs
Edukoppeling	Edukoppeling is een onderwijsspecifieke variant van Digikoppeling. De Edukoppeling-transactiestandaard maakt deel uit van de referentiearchitectuur voor het onderwijs (ROSA).
LAS	Leerling Administratie Systeem Het leerling administratiesysteem van de vo scholen vanuit waar de inschrijvingsgegevens worden verstuurd naar DUO
NORA	Nederlandse Overheids Referentie Architectuur Vanuit de NORA is de ROSA afgeleid
Onderwijsaanbieder	Een organisatie die door een bevoegd gezag is ingesteld voor het verzorgen van onderwijs
Onderwijslocatie	Een (cluster van) verblijfsobject(en) waar een onderwijsvolger zich kan inschrijven op opleidingen, die daar door een onderwijsaanbieder worden aangeboden
OSP	Onderwijs Service Poort: Dit is de infrastructurele component waarmee DUO middels webservices met ketenpartners communiceert (machine-machine koppeling). Het controleert of de aanroep technisch rechtmatig is en of de aanroep door een geauthentiseerde en geautoriseerde partij is verzonden.
PKI	Public Key Infrastructure: Is een samenstel van hardware, software, architectuur, organisatie, regels en procedures om digitale certificaten te creëren, distribueren, gebruiken, op te slaan of in te trekken.
RIO	Register Instellingen & Opleidingen Dit is het register van DUO waarin alle gegevens van Instellingen/scholen en opleidingen zijn vastgelegd.
ROSA	Referentie OnderwijsSector Architectuur: Is een afgeleide architectuur van de NORA, door het schakelpunt OCW opgesteld. Doelstelling is om binnen de onderwijssector gezamenlijk afspraken te maken die de informatie-uitwisseling tussen organisaties vergemakkelijkt. Daarnaast geeft de onderwijs referentiearchitectuur richting aan de ontwikkeling van een gemeenschappelijke ICT infrastructuur.

Term/afkorting	Omschrijving
SIS	Student Informatie Systeem Het administratiesysteem bij de onderwijsinstelling van waaruit gegevens over onderwijsaanbieders, onderwijslocatiegebruik en aangeboden opleidingen worden uitgewisseld met Rio.
SOAP	Simple Object Access Protocol. SOAP beschrijft een standaard om met webservices te werken. Het werkt via het principe van encapsulatie: het inpakken van berichten in een envelop. Deze berichten kunnen XML berichten zijn, maar ook RPC's (Remote Procedure Call) bevatten. SOAP is niet afhankelijk van de transportlaag en kan dus worden vervoerd over bestaande transportprotocollen, zoals: HTTP, JMS, FTP of SMTP. Op dit moment is HTTP de meest voorkomende transportbinding voor SOAP.
SSL/TLS	Secure Socket Layer/Transport Layer Security Encryptie-protocollen voor de beveiliging van communicatie over internet
UDDI	Universal Description, Discovery and Integration is een op XML gebaseerd register voor bedrijven (wereldwijd), waarmee het mogelijk is voor deze bedrijven om zichzelf en de diensten (webservices) die ze leveren, via het Internet te presenteren
UTC	een standaardtijd, gebaseerd op een atoomklok en gecoördineerd met de rotatie van de aarde.
VAVO	Voortgezet Algemeen Volwassenen Onderwijs
VO	Voortgezet Onderwijs
Webservice	Een webservice is een interface van een applicatie die een aantal functies biedt en aan te roepen is over het Internet, zonder menselijke tussenkomst.
WSDL	Web Service Description Language. WSDL kan worden gezien als de technische handleiding van een webservice waarin de functies en interfaces worden beschreven. Bijvoorbeeld de beschikbare functies die aangeroepen kunnen worden, welke invoerparameters worden verwacht en welke uitvoer terugkomt. Een of meer onderliggende XSD documenten bevat de daadwerkelijke definitie van de elementen in het bericht.
WUS	**W**sdl, **U**ddi, **S**oap: Het gekozen "koppelvlak standaard" binnen Digikoppeling. Het is het acroniem voor WSDL, UDDI en SOAP. WUS is voor de "bevragingen" (synchroon, request-response). Tegenhanger van EbMS (de andere standaard)
XML	Extensible Markup Language. XML is een verzameling regels, richtlijnen, gebruiken, voor het ontwerpen van tekstformaten voor gegevensuitwisselingen, op een dusdanige manier dat het eenvoudig is (voor de computer) bestanden te genereren en te lezen; bestanden, bovendien, die nooit ambigu zijn en waarmee vaak voorkomende fouten kunnen worden vermeden, zoals bestanden die niet extensibel zijn, die niet kunnen worden geïnternationaliseerd of vertaald of die platform-afhankelijk zijn.
XSD	XML Schema Definition Language, de beschrijving van de structuur en inhoud van XML berichten. Hierin staat o.a. hoe de elementen opgebouwd zijn en wat het formaat hiervan is (integer, binair, string etc.).

4. RIO webservices - algemeen

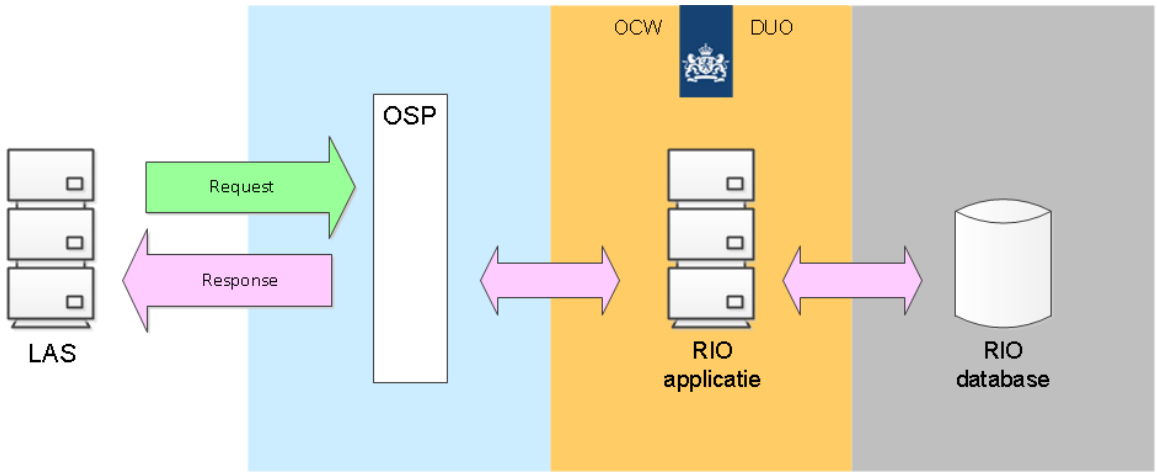
4.1. Inleiding

Rio kan via 2 kanalen beheerd worden:

- via webservices. Hiermee kunnen gegevens direct (zonder menselijke tussenkomst) met de systemen van scholen worden uitgewisseld. Een voorbeeld hiervan is de aanlevering van inschrijvingen aan DUO.
- via schermtransacties. Via de beveiligde site krijgt een medewerker van de scholen toegang tot een webapplicatie van DUO met op hem toegesneden functionaliteit, bv. Het beheren van contactgegevens van onderwijsaanbieders. Toelichting op het gebruik van deze schermen is te vinden op de beveiligde site.

Dit document beschrijft enkel de procesgang bij gebruik van webservices.

Voor alle RIO webservices geldt het synchrone interactiepatroon:



Synchrone uitwisseling betekent dat id's die uitgegeven worden door RIO bij nieuwe registraties ook synchroon teruggeleverd worden.

5. RIO webservices

De webservices hebben steeds betrekking op 1 van de 3 onderdelen van het onderwijsorganisatiedeel van RIO:

- Onderwijsaanbieders
- Onderwijslocatiegebruik
- Aangeboden Opleiding

De services zijn op te delen in 5 blokken die hieronder verder worden toegelicht.

1) Aanleveren nieuwe en gewijzigde gegevens
2) Raadplegen
3) Raadplegen hele organisatie
4) Raadplegen gewijzigde gegevens
5) Verwijderen

5.1. Aanleveren nieuwe en gewijzigde gegevens

Deze services hebben altijd betrekking op 1 object, dus bijvoorbeeld 1 onderwijsaanbieder of 1 aangeboden opleiding. Bij nieuwe opvoer van objecten waar RIO de sleutels voor uitgeeft worden deze sychroon door RIO teruggegeven.

5.2. Raadplegen

Deze services hebben altijd betrekking op 1 object, dus bijvoorbeeld 1 onderwijsaanbieder of 1 aangeboden opleiding.

5.3. Raadplegen hele organisatie

Deze services zijn bedoeld om de registratie van het SIS/LAS te toetsen tegen de registratie in RIO. Dit maakt het mogelijk om in de situatie dat er meerdere LASsen/SISsen zijn binnen een onderwijsaanbieder deze synchroon te houden met elkaar.

5.4. Raadplegen gewijzigde gegevens

Deze services zijn bedoeld om eigen registraties binnen het SIS/LAS actueel te houden. Alle nieuw opgevoerde, gewijzigde of verwijderde objecten sinds de vorige raadpleging kunnen worden opgehaald. Hiermee kan bijvoorbeeld gezorgd worden dat de schooladministratie altijd beschikt over een actuele lijst met de gegevens van alle onderwijsaanbieders.

5.5. Verwijderen

Deze services hebben altijd betrekking op 1 object, dus bijvoorbeeld 1 onderwijsaanbieder of 1 aangeboden opleiding. Een verwijdering is bedoeld voor het corrigeren van fouten door bijvoorbeeld een ten onrechte dubbel opgevoerde onderwijsaanbieder te verwijderen.

5.6. Gedetailleerde documentatie

De webservices zijn in detail gedocumenteerd in de bijbehorende documenten:

- “Webservice documentatie - DUO_RIO_Beheren_Raadplegen_OnderwijsOrganisatie_V1”.
- DUO_RIO_Beheren_Raadplegen_OnderwijsOrganisatie_V1.wsdl
- DUO_RIO_Beheren_Raadplegen_OnderwijsOrganisatie_V1.xsd

6. Technische aspecten van uitwisseling via webservices

6.1. Algemeen

Aansluiting op ~~de BRON-VO keten~~RIO gebeurt volgens de principes van Edukoppeling standaard. Uitwisseling vindt plaats op basis van de 1.2.1 standaard.

Voor meer informatie:
https://www.edustandaard.nl/standaarden/afspraken/afspraak/edukoppeling/1.2/

Voor de koppelingen wordt gebruik gemaakt van de Edukoppeling WUS 1.2 standaard.

Voor meer informatie:
https://www.edustandaard.nl/fileadmin/edustandaard/Bestanden/Afspraken/Edukoppeling/Edukoppeling_Transactiestandaard_1.2__definitief_.pdf

We maken in de BRON-VO keten gebruik van het Edukoppeling 2W-BE-S profiel, wat wil zeggen dat er gewerkt wordt met SOAP berichten die over een 2 zijdig TLS transportbeveiliging kanaal uitgewisseld worden. Daarbij wordt gebruik gemaakt van berichtsigning met behulp van WS-Security 1.0. Dit om de ontvanger van het bericht te garanderen dat het bericht vanaf de afzender niet ingezien maar ook niet aangepast kan worden. Zowel de body, ws-security timestamp als de wsa:headers moeten worden gesigned.

Partijen worden uniek geïdentificeerd aan de hand van een OIN (Overheids identificatie nummer). Het OIN bestaat altijd uit 20 posities en bestaat uit een aantal vaste onderdelen: "de prefix", "hoofdnummer" en "suffix". Bijvoorbeeld '00000007'(prefix) + de BRIN (3 voorloopnullen, BRIN = 4 posities + 00, hoofdnummer) + het administratienummer (3 posities, suffix). Bijvoorbeeld 00000007000025MB00000. Het OIN van voor het afgeleide administratiepunt komt er als volgt uit te zien: "00000007000025MB00**003**". Het administratienummer mag in principe door de instelling/SAAS-leverancier zelf worden bepaald. Dit nummer moet echter wel uniek zijn per BRIN binnen de keten. Tevens moet het nummer doorgegeven worden aan DUO. Op basis van het OIN worden endpoints aan de instellingen gekoppeld.
Bovenstaande opbouw beschrijft een OIN op basis van een BRIN nummer. OIN kunnen op meerdere manieren worden opgebouwd. De prefix zal dan vershillen. Een OIN op basis van het KvK nummer zal de volgende prefix bevatten: "00000003
". Een software leverancier zal dit nummer bijvoorbeeld kunnen gebruiken voor de uitwisseling. Zij beschikken immers niet over een BRIN.

De suffix binnen het OIN bestaat in principe uit de '000' waarde. Tenzij er binnen een instellingen meeerdere administratiepunten of leveranciers actief zijn. Elk administratiepunt zal dan in gezamenlijk overleg een andere suffix gebruiken in het OIN om de uitwisseling met DUO en eventuele andere ketenpartners mogelijk te maken. Het OIN is terug te vinden in de technische laag van de berichtuitwisseling, de zogenaamde wsa:to en wsa:from headers.

Voor DUO geldt het volgende OIN 00000001800866472000.
Zie https://register.digikoppeling.nl/home/index voor het overzicht van de uitgegeven OIN's.

Wat houdt dit in de praktijk in?

Als eerste moeten vooraf de publieke certificaten tussen aanbieder en afnemer van de koppelvlakken uitgewisseld worden. Op basis van de eigen private key wordt namelijk een bericht ondertekend, aan de kant van de aanbieder van de service moet m.b.v. de bijbehorende public key de signing gecontroleerd worden.

6.1.1. Beveiligingseisen

Uitgangspunt is dat de aanlevering van de gegevens van de scholen aan DUO geen persoonsgegevens bevatten.

NB: De scholen zullen zelf adequate beveiligingsmaatregelen moeten treffen met betrekking tot de (lokale) identificatie, autorisatie, controle, logging welke opgenomen kunnen worden in het LAS/SIS en eigen verantwoordelijkheid moeten nemen voor de lokale beveiliging. Specifieke maatregelen op het gebied van de lokale beveiliging worden door DUO niet voorgeschreven en zijn daarom geen onderdeel van dit PvE.

6.1.2. Externe hosting

Met betrekking tot een hostingspartner binnen de EU, wordt het aangeraden om een bewerkingsovereenkomst af te sluiten. Een hostingpartner buiten de EU is niet toegestaan zonder afstemming met DUO.
Een model bewerkingsovereenkomst kan op onderstaande link worden gevonden.

https://www.pianoo.nl/sites/default/files/documents/documents/model-bewerkersovereenkomstarvodi.pdf

6.1.3. Certificaten

Als gevolg van de keuze voor het Edukoppeling profiel wordt er gebruik gemaakt van een 2-zijdige TLS verbinding. De client (de verzender van het bericht) en de server (de partij die het bericht ontvangt van de client) moeten zichzelf authentiseren alvorens er tot berichtuitwisseling wordt overgegaan. Deze tweezijdige TLS verbinding garandeert dat beide partijen zijn wie ze zeggen te zijn.

Conform de edukoppeling 1.2 standaard wordt alleen TLS versie 1.2 toegestaan. Het is niet mogelijk om een verbinding met DUO tot stand te brengen op basis van de SSL Of TLS 1.0/1.1 standaard.

DUO accepteert naast de PKI Overheidscertificaten (https://cert.pkioverheid.nl/) Ook de door haar zelf uitgegeven ODOC certificaten.
Zie Bijlage I: Aanvraagprocedure ODOC Certificaten~~Bijlage 14I: Aanvraagprocedure ODOC Certificaten~~ voor de aanvraagprocedure van deze certificaten.
Certificaten hoeven niet bekend te worden gemaakt bij DUO. Aan DUO zijde worden PKI Overheid en ODOC certificaten vertrouwd.
De aan te sluiten instelling/leverancier moet echter wel bij DUO worden aangemeld om de autorisatie tot de gewenste webservice te regelen en de nodige firewall(s) open te laten zetten.

6.2. Technische aanroep van de webservice

Een webservice is een applicatie die een aantal functies biedt en aan te roepen is over het Internet. De in- en output van deze functies gebeurt voornamelijk in XML-formaat en volgens vaste afspraken. Deze afspraken zijn platformonafhankelijk; iedere webservice kan vanaf ieder soort platform (Unix, Windows-NT, etc.) worden gebruikt.

De code achter een webservice kan gemaakt zijn met alle mogelijke middelen. Of het nu Java is, C# of een scriptingtaal, het kan allemaal een webservice bieden. Een applicatie

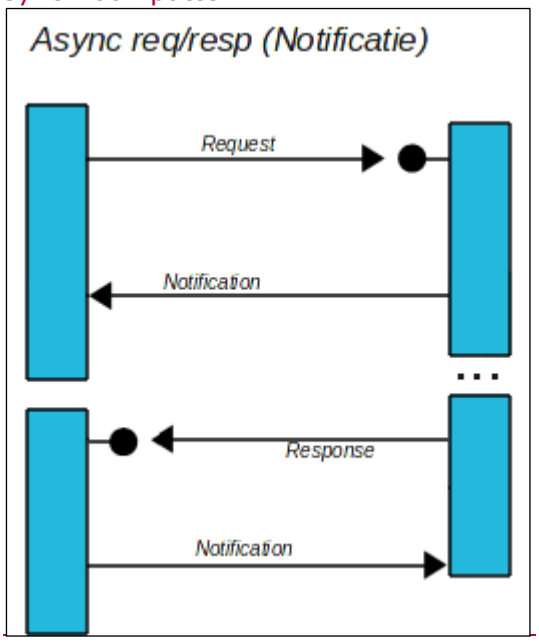
biedt een webservice omdat de interface zich houdt aan bepaalde afspraken. Alle webservices spreken dezelfde taal, over hetzelfde protocol, met vaste afspraken over het formaat.

De definitie van een webservice ligt vast in een WSDL (Web Service Description Language). In de WSDL staat beschreven welke services DUO aanbiedt en de locatie van de service.

Na het uitvoeren van de stappen Identificatie (welke partij wil een bericht sturen), Authenticatie (is dit daadwerkelijk de partij die geïdentificeerd is) en Autorisatie (mag deze partij de service gebruiken) zal er een XSD controle op de payload/body van het SOAP bericht uitgevoerd worden. Voldoet het bericht niet aan de XSD controle of wordt in een van omschreven stappen een fout geconstateerd, dan zal er via een SOAP-fault bericht aangegeven worden dat het serviceverzoek niet verwerkt kon worden. De verzender van het bericht zal hierop passende maatregelen moeten nemen om ervoor te zorgen dat het bericht alsnog verwerkt kan worden. Er zal in deze gevallen altijd een nieuwe aanlevering uitgevoerd moeten worden om het bericht alsnog verwerkt te krijgen.

6.3. Uitwisselpatronen

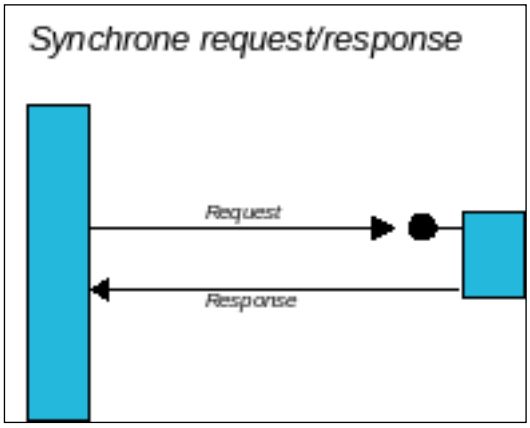
Uitwisseling van het berichtenverkeer vindt plaats volgens onderstaand ~~a~~synchroon request/response ~~met notificatie~~ pattern. ~~Een betere naam hiervoor is: 'dubbel' synchroon pattern.~~



~~De service-requestor (partij A) doet een verzoek. Er volgt hierop alleen een ontvangstbevestiging van de service-provider (partij B).~~

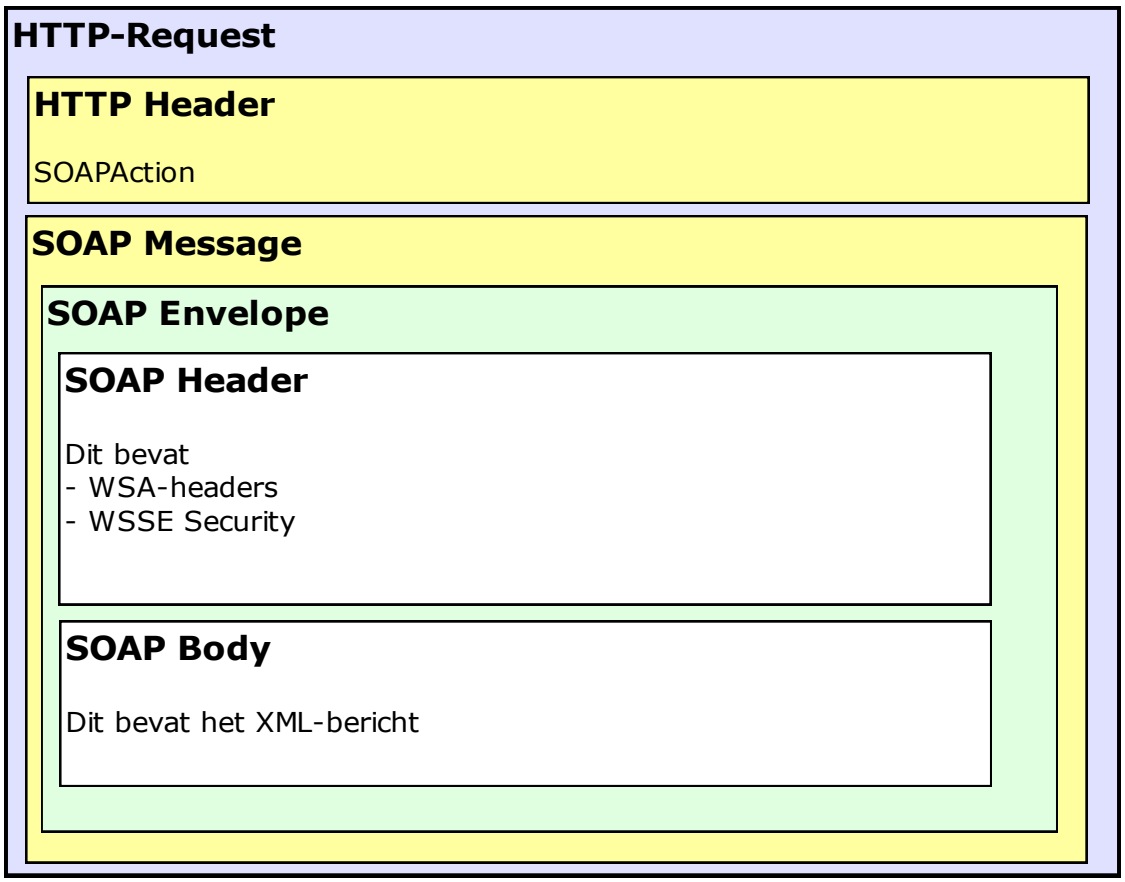
~~Na de verwerking van het verzoek aan de kant van de service-provider (partij B) wordt er door deze partij een service aangeroepen bij partij A met het verwerkingsresultaat. Partij A stuurt daarop een ontvangstbevestiging naar partij B.~~

~~Ook bij de spontane berichten die vanuit DUO verstuurd worden is een ontvangstbevestiging vereist.~~



6.4. Soap berichtenstructuur

Elke aanroep van een service bestaat uit een SOAP-header (de stuurgegevens) en een SOAP-body (de berichtgegevens). In de SOAP-body staat het te verzenden bericht (request) of het antwoord (response). Bij ieder bericht wordt in de body een bedrijfsdocument element meegegeven waarin metagegevens over de levering wordt meegegeven.



Voor een voorbeeld van een bericht zie **Fout! Verwijzingsbron niet gevonden.**~~Bijlage 15: Voorbeeld berichten~~

6.4.1. Gebruikte karakterset

Digikoppeling schrijft in het uitgangspunt WS006 dat alleen UTF-8 wordt ondersteund.

6.4.2. HTTP-headers

De http header: "SOAPAction" moet worden gevuld met de namespace + operatie. Deze komt exact overeen met de waarde in de wsa:Action, bijvoorbeeld:

"http://duo.nl/contract/DUO_RIO_Beheren_Raadplegen_OnderwijsOrganisatie_V1/aanleveren_onderwijsaanbieder"

Daarnaast moet in de http header: "Content-Type" worden aangegeven welke karakterset gebruikt wordt. Een andere karakterset dan UTF-8 zal worden afgekeurd.

"Content-Type text/xml;charset=UTF-8"

6.4.3. Timestamp

Toevoegen van de timestamp is verplicht gesteld bij het aanleveren van VO berichten. Als de timestamp niet (correct) wordt meegegeven, wordt dit terug gemeld als foutmelding.

```
<wsu:Timestamp wsu:Id="TS-120D1F5A29709C812D149699419570340">
<wsu:Created>2017-06-09T07:43:15.703Z</wsu:Created>
<wsu:Expires>2017-06-09T09:06:35.703Z</wsu:Expires>
</wsu:Timestamp>
```

6.4.4. Lege velden

Lege optionele velden in een XML bericht, dienen te worden weglaten uit het bericht. Een XML-tag zonder inhoud mag niet verstuurd worden.

6.4.5. IdentificatiecodeBedrijfsdocument

Het veld "identificatiecodeBedrijfsdocument" in de berichten moet worden gevuld met een correct en uniek UUID. Dit veld wordt binnen de hele keten gebruikt als track & trace-id. Niet unieke UUID's worden afgekeurd.

6.4.6. TLS

Volgens de edukoppeling standaard kan alleen gebruik worden gemaakt van TLS 1.2. Oudere versies en SSL varianten worden niet geaccepteerd.
Op de binnengekomen certificaten moeten de volgende validaties worden uitgevoerd:

- Expiratie certificaat
  Hierbij wordt gecontroleerd of de einddatum in het certificaat nog niet verlopen is.
- Revocatie van de hiërarchie
  Hierbij wordt gecontroleerd of het certificaat niet is ingetrokken door de certificaat-autoriteit die het certificaat heeft uitgegeven.
- Verificatie van de hiërarchie
  Hierbij wordt gecontroleerd of het certificaat overeenkomt met het verwachte certificaat

Voor de versleuteling worden onder andere de volgende ciphers door DUO geaccepteerd. DUO accepteert alleen ciphers op basis van minimaal 128 bits encodering. Ciphers op basis van "RC4", "MD5" of "3DES" worden niet geaccepteerd.

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

6.4.7. Signing

De volgende gegevens worden gesigned:

- timestamp in de header
- WSA-velden in de header, elk WSA veld moet apart gesigned zijn. Signing van de WSA headers wordt afgedwongen aan DUO zijde.
- SOAP body
- "Binarysecuritytoken" moet worden toegevoegd aan de signing.
- Signing moet minimaal voldoen aan de SHA-2 standaard. SHA-1 wordt niet langer als veilig beschouwd/toegestaan.

DUO maakt voor de terugkoppeling van berichten gebruik van haar eigen certificaat. Public key kan worden aangevraagd bij DUO.

Certificaatdetails DUO Test-omgeving:
Subject:
C=NL, ST=Groningen, L=Groningen, O=Dienst Uitvoering Onderwijs, OU=AIB, serialNumber=00000001800866472000, CN=xml-test.duo.nl
Issuer:
C=NL, O=KPN Corporate Market BV, CN=KPN Corporate Market CSP Organisatie CA - G2

Certificaatdetails DUO Productie-omgeving:
Subject:
C=NL, ST=Groningen, L=Groningen, O=Dienst Uitvoering Onderwijs, OU=TAB, serialNumber=00000001800866472000, CN=webservice.duo.nl
Issuer:
C=NL, O=KPN Corporate Market BV, CN=KPN Corporate Market CSP Organisatie CA - G2

De complete (productie) 'certificate chain' kan (indien nodig) worden verkregen via deze website: https://cert.pkioverheid.nl/

6.4.8. WSA-headers

In de berichtuitwisselingen moeten diverse ws-addressing headers gezet worden, dit betreft de volgende items voor respectievelijk het request en het bijbehorende response.

Op de WSA-headers in zowel het requestbericht als het responsebericht moeten de volgende validaties worden uitgevoerd:

- From en To moeten een OIN bevatten; Hierbij is het van belang dat het OIN wordt toegevoegd na de tag: "oin=". Als het OIN niet correct wordt toegevoegd is DUO niet in staat om deze uit te lezen.
- De To moet bij een aanlevering het OIN bevatten van DUO (00000001800866472000), zie ook onderstaand voorbeeld.
- wsa:Action moet overeenkomen met de http header: "SOAPAction", hier moet namespace + operatie in worden opgevoerd.
- MessageID moet gevuld zijn
- De verschillende WSA headers moeten net zoals de timestamp en de body van het bericht ondertekend worden.

1.1.1.1 WSA-headers Request

Veld	wsa: To
Inhoud	Vullen met WSDL-Adres uit de soapaction +OIN responder
Voorbeeld	<wsa:To> http://www.w3.org/2005/08/addressing/anonymous?oin=00000001800866472000 </wsa:To>

Veld	wsa: Action
Inhoud	vullen met namespace + WSDL-Operatie
Voorbeeld	<wsa:Action> http://duo.nl/contract/DUO_VOAanlevering_InschrijvingVo_V1/aanleverenInschrijvingVo </wsa:Action>

Veld	wsa:MessageID
Inhoud	vullen met unieke UUID
Voorbeeld	<wsa: MessageID > urn:uuid:550e8400-e29b-41d4-a716-446655440000 </wsa:MessageID>

Veld	wsa:From
Inhoud	vullen met 'Anonymous' +OIN requester
Voorbeeld	<wsa:From> <wsa:Adress> http://www.w3.org/2005/08/addressing/anonymous?oin=0000000700025MB00000 </wsa:Adress> </wsa:From>

NB: het wsa:MessageId hoeft NIET hetzelfde UUID te bevatten als het functionele veld "identificatiecodeBedrijfsdocument". Het identificatiecodeBedrijfsdocument kan gebruikt worden ter identificatie van de functionele berichtstroom, het wsa:MessageID is een unieke identificatie van het technisch bericht.

1.1.1.2 WSA-headers Response

Veld	wsa: To
Inhoud	Vullen met 'Anonymous' + OIN requester
Voorbeeld	<wsa:To> http://www.w3.org/2005/08/addressing/anonymous?oin=0000000700025MB00000 </wsa:To>

Veld	wsa: Action
Inhoud	vullen met namespace + WSDL-Operatie
Voorbeeld	<wsa:Action> http://duo.nl/contract/DUO_VOAanlevering_InschrijvingVo_V1/aanleverenInschrijvingVo </wsa:Action>

Veld	wsa:RelatesTo
Inhoud	vullen met MessageID van het request (UUID)
Voorbeeld	<wsa:RelatesTo> urn:uuid:550e8400-e29b-41d4-a716-446655440000 </wsa:RelatesTo>

Veld	wsa:From
Inhoud	vullen met 'Anonymous' + OIN requester
Voorbeeld	<wsa:From> <wsa:Address> http://www.w3.org/2005/08/addressing/anonymous?oin=00000001800866472000 </wsa:Address> </wsa:From>

6.5. Foutafhandeling

Binnen de edukoppeling 1.2 standaard zijn onderstaande foutcodes gedefinieerd.
Deze foutsituaties worden vaak veroorzaakt door fouten in de programmacode. Om deze fouten snel op te sporen zijn de foutcodes zo specifiek mogelijk gemaakt. Hierbij gaan specifieke codes altijd boven algemenere codes (dus bv EK0023 gaat boven DK0011).

Overzicht foutcodes:

Faultcode	FaultString	Toelichting	Aandachts-punt
VersionMismatch .DK0001	Invalide envelope	Het bericht heeft een invalide envelope namespace (voldoet niet aan de SOAP 1.1 specificatie)	*1
Client.DK0002	Niet geautoriseerd	Client is niet geautoriseerd om deze aanroep te doen	
Client.DK0003	Invalide soap-action	Ongedefinieerde actie of anderszins onjuist gevuld. N.B. Het gaat hier om de SOAPAction n het HTTP-request, niet om de wsa:Action	*1
Client.DK0004	Niet conform XSD	Bericht is niet conform de afgesproken specificatie. Details over de fout kunnen opgenomen worden in het 'detail' veld	
Client.DK0005	Wsa:To ontbreekt	Veld is verplicht	
Client.DK0006	Wsa:Action ontbreekt	Veld is verplicht	
Client.DK0007	Wsa:MessageID ontbreekt	Veld is verplicht	
Client.DK0008	Wsa:RelatesTo ontbreekt	De relatie naar een eerder bericht wordt verwacht wordt, maar is niet aanwezig	*2
Client.DK0009	Niet conform UTF-8	Bericht bevat tekens die niet voldoen aan de UTF-8 spec	*1
Client.DK0010	Andere headers	Bericht bevat headers anders dan de WS-Addressing	*3
Client.DK0011	Onjuiste waarde in wsa header	Bericht bevat 1 of meer WS-Addressing velden die niet voorgeschreven worden of foutieve waarde bevatten	*3
Client.EK0020	Wsa:From ontbreekt	Veld is verplicht	
Client.EK0021	Wsa:From bevat geen geldig OIN	Controle op syntax	

Faultcode	FaultString	Toelichting	Aandachts-punt
Client.EK0022	Wsa:To bevat geen geldig OIN	Controle op syntax	
Client.EK0023	Wsa:MessageID bevat geen UUID	Controle op syntax	
Client.EK0030	OIN in TLS certificaat ontbreekt of is ongeldig	De client moet de verbinding opzetten met een digikoppeling compliant PKI-overheid of PKI-ODOC certificaat	
Client.EK0031	Berichtondertekening niet aanwezig of onjuist	Het bericht moet volgens contract ondertekend worden maar de ondertekening is ongeldig of niet aanwezig	
Server.DK0050	Service afhandeling geeft fout	Het proces dat het serviceverzoek moet afhandelen geeft een fout	*4
Server.DK0051	Service niet beschikbaar	Het proces dat de service moet afhandelen is niet beschikbaar of geeft een time-out	

Aandachtspunten

*1) Het is verplicht foutafhandeling volgens bovenstaande codes te implementeren. Soms is het binnen specifieke implementaties echter onmogelijk bepaalde codes terug te geven, bijvoorbeeld omdat de implementatie van een controle op protocol- of infrastructureel niveau uitgevoerd wordt.
Binnen DUO geldt dit voor codes DK0001, DK0003 en DK0009. De client moet in dit geval om kunnen gaan met afwijkende of meer generieke foutcodes (bv Faultcode:Client, of een HTTP-statuscode in de 500 range)

*2) De functionaliteit bepaalt wanneer een relatesTo verplicht is. Omdat het echter om een logistiek gegeven gaat in de wsa-headers is er toch voor gekozen om hiervoor een standaard foutcode op te nemen.

*3) Formeel voldoet een bericht niet aan de afspraken maar als dit gedrag niet onderdrukt kan worden door een client, dan hoeft dit niet te leiden tot een foutsituatie. De (ontvangende)service mag deze informatie echter niet gebruiken voor het logistiek routeren van het bericht.

*4) In de 'faultstring' van het error bericht wordt de functionele foutmelding teruggekoppeld van de volgende fouten:
- Fout in de waardenlijst
  Een voorbeeld van deze fout is:
  "Ongeldige waarde voor naam: ExperimentX"
- Ongeldige waarde in het veld identificatie bedrijfsdocument
  Een voorbeeld van deze fout is:
  "Ongeldige waarde voor identificatiecodeBedrijfsdocument"

Voor een voorbeeld van een foutbericht zie **Fout! Verwijzingsbron niet gevonden.**~~Bijlage 15: Voorbeeld berichten~~

7. Bijlage I: Berichtdefinities - algemeen

De onderstaande beschrijving van berichten is met name bedoeld om inzicht te geven in welke gegevens worden uitgewisseld. De berichtstructuur is technisch uitgewerkt in een XSD per service. Bij eventuele afwijkingen tussen de beschrijving hieronder en de XSD is het XSD altijd leidend.

7.1. Inleiding

7.1.1. Beschrijving van de berichten

In de beschrijving van de berichten worden sleutelvelden grijs gearceerd en onderstreept aangegeven.

Per element wordt het formaattype beschreven aan de hand van de types in de onderstaande tabel. Voor de exacte formaattypen (patterns e.d.) dient het XSD te worden geraadpleegd.

Formaattype	Betekenis	Voorbeeld
AN	Alfanumerieke waarde Voor de te gebruiken tekenset zie § 6.4.1~~4.4.1~~.	Dfe54.dea**9
AN5	Een attribuut met een maximale veldlengte van 5 tekens. NB. De formaten AN1 en AN1..1 hebben dezelfde betekenis. Daarom wordt enkel het formaat AN1 gebruikt. Hetzelfde geldt voor AN1..5 en AN5. Ook hier wordt enkel AN5 gebruikt.	A AB AB- AB-1 AB-12
AN5..5	Een attribuut met een minimale en maximale veldlengte van 5 tekens.	AB-12
N	Numerieke waarde	125635
Boolean (XML-berichten)	Booleanwaarde (zoals gebruikt in de elektronische berichten-uitwisseling)	"false" (niet waar) "true" (waar)
Boolean (bestanden)	Booleanwaarde (zoals gebruikt in de bestandsuitwisseling)	"J" (waar) "N" (niet waar)

Alle datumvelden zijn geïmplementeerd als alfanumeriek veld. In de onderstaande tabel is beschreven hoe hiermee omgegaan dient te worden.

Formaattype datum	Betekenis	Voorbeeld
D	Tijdbepaling van datum in jaar, maand en dag	2012-04-23
AN8..8 (bestanden)	Tijdbepaling van datum; bestaat uit 4 cijfers voor het jaar, 2 cijfers voor de maand en 2 cijfers voor de dag. (zoals gebruikt in de bestandsuitwisseling)	20120423
AN10..10	Tijdsbepaling van datum; bestaat uit 4 cijfers voor het jaar, een streepje, 2 cijfers voor de maand, een streepje en 2 cijfers voor de dag. Een onvolledige datum is mogelijk. De dag mag 00 zijn, of de maand en de dag mogen 00-00 zijn.	2012-04-23 2012-00-00 2012-05-00

Formaattype datum	Betekenis	Voorbeeld
AN19	Tijdsbepaling van datum en tijd in jaar, maand, dag, uur, minuten, seconden; bestaat uit 4 cijfers voor het jaar, een streepje, 2 cijfers voor de maand, een streepje en 2 cijfers voor de dag, een T voor de tijdaanduiding, 2 cijfers voor de uren, een dubbele punt, 2 cijfers voor de minuten, een dubbele punt, 2 cijfers voor de seconden	2012-01-30T22:07:50
AN19..29	Bestaat uit 4 cijfers voor het jaar, een streepje, 2 cijfers voor de maand, een streepje en 2 cijfers voor de dag, een T voor de tijdaanduiding, 2 cijfers voor de uren, een dubbele punt, 2 cijfers voor de minuten, een dubbele punt, 2 cijfers voor de seconden, een punt en drie cijfers voor duizendste van seconden, een plusteken, 2 cijfers voor uren tijdsverschil (t.o.v. UTC), een dubbele punt en 2 cijfers voor minuten tijdsverschil (t.o.v. UTC). Indien er een datum/tijd wordt aangeleverd zonder milliseconden, dan zal DUO dit als ".000" interpreteren. Indien er een datum/tijd wordt aangeleverd zonder afwijking t.o.v. de UTC, dan zal DUO dit interpreteren als de lokaal geldende tijd. Dit betekent dat dit in de winter geldt als UTC+01:00 en tijdens zomertijd als UTC+02:00 (respectievelijk 1 en 2 uur later dan de standaardtijd).	2012-03-16T14:58:22 2012-03-16T14:58:22.831 2012-03-16T14:58:22.831+02:00

Velden met waardenlijsten zijn allemaal van hetzelfde type ('WaardenlijstType') en zijn daarmee allemaal 70 karakters lang. Om te voorkomen dat het problemen oplevert wanneer de veldlengte voor deze velden daadwerkelijk volledig wordt benut is per veld afgesproken wat de maximaal gewenste lengte is. In de onderstaande beschrijving is deze (gewenste) lengte opgenomen.
Het gebruik van hoofd- en kleine letters voor waarden uit waardenlijsten dient gelijk te zijn (mag niet afwijken) van de waarden zoals deze in dit document zijn beschreven.

7.1.2. Controles

In een los bijgevoegd document zijn de controles beschreven die uitgevoerd worden nadat een levering door DUO is ontvangen en DUO een ontvangstbevestiging naar de instelling heeft gestuurd. (Zie paragraaf 1.3 over bijbehorende documenten)

Voordat de ontvangstbevestiging wordt verstuurd worden echter ook al een aantal technische controles uitgevoerd op formaat en vaste waardenlijsten. Ook kunnen er onverwachte technische omstandigheden optreden waardoor het bericht wordt afgekeurd. Deze technische foutafhandeling wordt beschreven in het hoofdstuk "foutafhandeling". Voorbeelden van fouten in het formaat en vaste waardenlijsten zijn:

- In de opleidingscode staan letters in plaats van cijfers;
- Datum uitschrijving bevat een ongeldige datum (bijv. 31 november);

Algemeen geldt voor de functionele controles dat ze worden uitgevoerd in de volgorde waarin ze in de tabellen bij het betreffende bericht genoemd staan.

7.1.3. Bedrijfsdocument

Ieder bericht gaat vergezeld van een zogenaamd bedrijfsdocument. De gegevens uit het bedrijfsdocument hoeven slechts éénmaal per bericht te worden opgenomen en zijn bedoeld om informatie over het bericht door te geven.

De inhoud van de attributen *verzendendeInstantie* en *ontvangendeInstantie* uit het request worden in de response die wordt teruggestuurd omgewisseld; de inhoud van *verzendende instantie* uit het request komt dus in *ontvangende instantie* van de response te staan en de inhoud van *ontvangende instantie* uit het request in *verzendende instantie* van de response.

~~**Verwerkingsvolgorde van berichten die een register muteren**~~
~~Het attribuut *datumTijdBedrijfsdocument* wordt gebruikt om na te gaan of de berichten in chronologische volgorde worden verwerkt. Het is technisch mogelijk dat berichten elkaar inhalen. Daarom wordt hier bij het verwerken van gegevens (nieuwe aanleveringen, wijzigingen en verwijderingen) rekening mee gehouden. Afhankelijk van de *datumTijdBedrijfsdocument* wordt nagegaan of een bericht de meeste actuele gegevens bevat. Indien dit het geval is, worden de gegevens overgenomen. Bevat een register gegevens die meer recent zijn dan de *datumTijdBedrijfsdocument*, dan worden deze gegevens niet overgenomen; ze zijn dan immers inmiddels verouderd. Wanneer hier sprake van is, wordt dit teruggemeld.~~

Naam	Verplicht	Formaat	Definitie
identificatiecodeBedrijfsdocument	Ja	AN36	Gegevens aan de hand waarvan een bericht kan worden geïdentificeerd. De identificatiecode moet uniek zijn in de vorm van een UUID (zie http://nl.wikipedia.org/wiki/Universally_unique_identifier). De identificatiecode uit de request zal in de ontvangstbevestiging overgenomen worden. De identificatiecode wordt ook weer opgenomen in de request van de terugkoppeling en de ontvangstbevestiging daarvan. **Toelichting:** Bestaat verder uit letters, cijfers, underscore, backslash of verbindingsstreepje. De identificatiecode wordt als track & tracecode door de hele keten (inclusief bekostiging) van school en DUO gebruikt. Dit gegeven moet uniek zijn.
verzendendeInstantie	Ja	AN3..22	De instantie die een bedrijfsdocument heeft verzonden. Hierin staat de identificatie van de onderwijsaanbieder van de onderwijsaanbieder als het bericht van de school naar DUO verstuurd wordt of "DUO" als het bericht van DUO naar de school verstuurd wordt.

Naam	Verplicht	Formaat	Definitie
ontvangendeInstantie	Ja	AN3..22	De instantie voor wie bedrijfsdocument is bestemd. Hierin staat de tekst "DUO" als het bericht van de school naar DUO verstuurd wordt of de identificatie van de onderwijsaanbieder van de onderwijsaanbieder als het bericht van DUO naar de school verstuurd wordt.
datumTijdBedrijfsdocument	Ja	AN24..29	Datum en tijdstip waarop het bericht is aangemaakt, weergegeven in UTC. ~~**Toelichting:**~~ ~~Deze datum en tijdstip worden onder meer gebruikt voor bepaling van volgordelijkheid bij verwerking van onderwijsdeelnames en -resultaten~~

7.1.4. Terugkoppeling

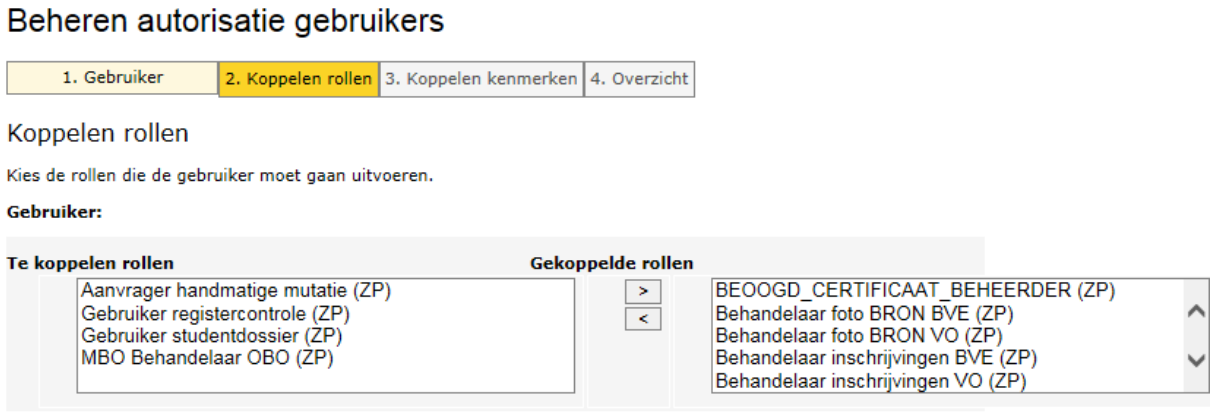
De meeste terugkoppelingen bevatten het volgende generieke element dat hier eenmalig wordt beschreven.

Naam	Verplicht	Formaat	Definitie
leveringGoedgekeurd	Ja	Boolean	Indicatie of een gegevenslevering is goedgekeurd
Foutmelding, 0..1 keer			
foutcode	Ja	AN60	Identificerende code voor een specifieke functionele foutsituatie
fouttekst	Ja	AN200	Uitleg van een functionele foutsituatie
Sleutelgegeven, 0..5 keer per Foutmelding			
Sleutelnaam	Ja	AN25	Naam van het sleutelgegeven
Sleutelwaarde	Ja	AN25	De waarde van het sleutelgegeven

8. Bijlage ~~I~~I: Aanvraagprocedure ODOC Certificaten

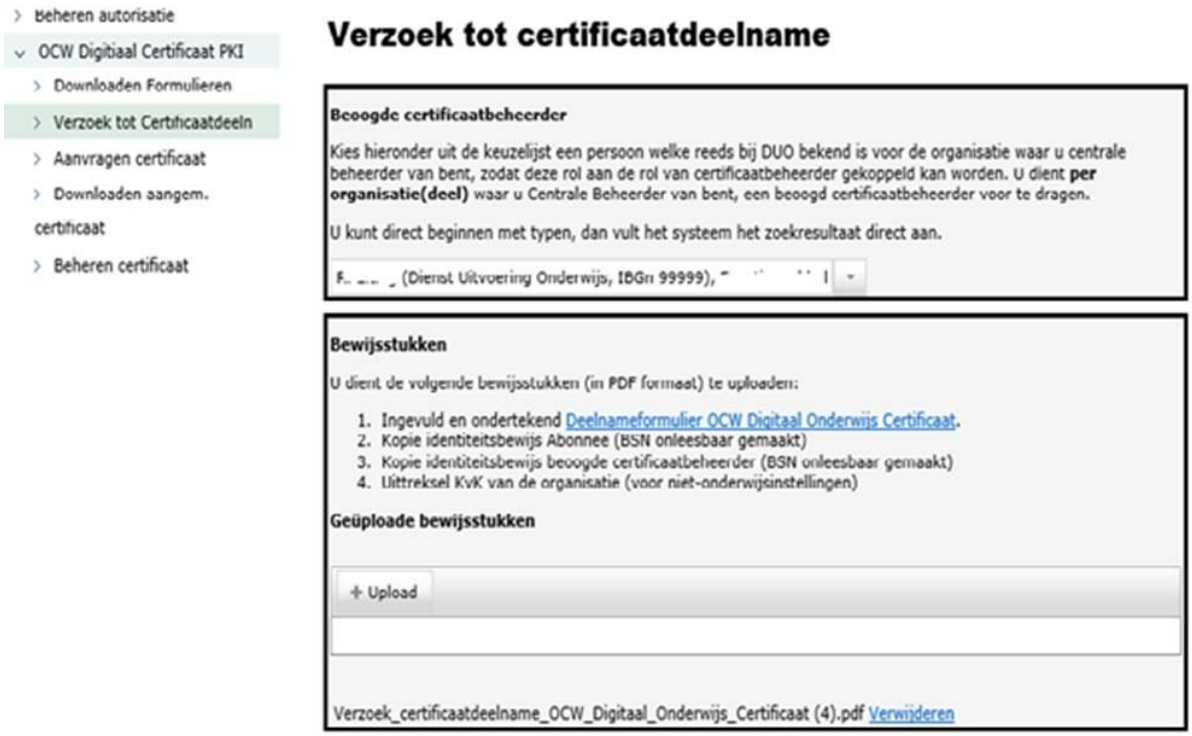
Voordat certificaten kunnen worden aangevraagd, moet een certificaatbeheerder bekend worden gemaakt bij DUO. Dit proces verloopt via het zakelijk portaal op de productieomgeving. Nadat een certificaatbeheerder is aangemeld kunnen zowel certificaten voor de veldtest als voor de productieomgeving worden aangevraagd. Het aanmelden van personen als certificaatbeheerder dient te worden uitgevoerd door de aangestelde beheerder bij de betreffende instelling.

Stap 1 is het koppelen van de rol, beoogd certificaatbeheerder via het zakelijk portaal, zie onderstaande afbeelding.



Na het koppelen van de betreffende rol aan de gewenste certificaatbeheerder moeten de nodige bewijsstukken worden aangeleverd via onderstaande transactie. Het is van belang om de gegevens correct aan te leveren, anders zal de aanvraag worden afgewezen en moet deze opnieuw worden ingediend.

1. Komen de gegevens onder 1. Gegevens Abonnee overeen met het identiteitsbewijs abonnee.
2. Komen de gegevens onder 2. Gegevens Organisatie overeen met de instellingsinformatie op duo.nl (of voor niet-onderwijsinstellingen op kvk.nl, aan de hand van de kopie KVK register)[1].
3. Komen de gegevens onder 3. Gegevens certificaatbeheerder overeen met het identiteitsbewijs certificaatbeheerder.
4. Zijn de vraag en het antwoord onder 4. Identiteitscontrole en ondertekening leesbaar.
5. Komen de handtekeningen overeen met die op de identiteitsbewijzen.



Aanvraagprocedure ODOC certificaten veldtest
Certificaten voor de veldtest moeten via de mail worden aangevraagd, door de aangemelde certificaatbeheerder. De certificaatbeheerder kan een csr bestand aanleveren. Hierin mogen geen velden worden leeg gelaten.

“
Common name: webservice.duo.nl
Organization: DUO
Organizational unit: DUO
City/locality: Groningen
State/province: Groningen
Country: NL
Email: duo@duo.nl
”

Daarnaast worden bij de testcertificaten een aantal velden door DUO vastgestelde waarden overschreven. Organisatie is hier een van.

Het aan te leveren CSR bestand kan via onderstaande website worden gevalideerd. Hier mogen geen fouten of waarschuwingen naar voren komen.

https://cryptoreport.websecurity.symantec.com

Aanvraagprocedure ODOC certificaten productie
ODOC productiecertificaten moeten via een transactie in het zakelijk portaal worden aangevraagd.
Ook via het zakelijk portaal kan een csr bestand worden aangeleverd.

Voor de productiecertificaten vindt er een controle plaats op de opgegeven commen name in het certificaat.
Mochten de gegevens van de houder van de domeinnaam niet overeenkomen met de opgegeven common name in het certificaat moet vooraf contact gezocht worden met DUO, om afkeur te voorkomen.

Het is helaas niet mogelijk om een afgewezen certificaatverzoek te heropenen. Als er fouten in het csr bestand staan, of afwijkingen in de aanvraag, zal deze opnieuw moeten worden ingediend via het portaal.