SION
Dienst Uitvoering Onderwijs

Edukoppeling

Transactiestandaard

Versie 1.1

Datum: 27 maart 2014

Inhoudsopgave

Hoofdstuk 1 Inleiding

§ 1.1 Aanleiding

Deze standaard is geïnspireerd door de recente toename van de hoeveelheid service- en berichtenverkeer zowel naar volume als naar type binnen het onderwijsveld en tussen de overheid en het onderwijsveld. Vaak worden afspraken op infrastructureel gebied gemaakt voor één bepaalde toepassing.

Het Strategisch Informatiebeleidplan 2013-2016 van OCW heeft als doel een kwalitatief hoogwaardige en toekomstvaste informatievoorziening te realiseren. Er is een programmalijn onderkend met een omslag van de traditionele scheiding tussen onderwijsveld en overheid naar een gemeenschappelijke infrastructuur. In 2012 en 2013 is daaraan concreet gewerkt in het programma SION van onderwijsraden, Kennisnet en Surf en het Schakelpunt OCW van de Dienst Uitvoering Onderwijs (DUO).

Ook de overheid werkt sinds 2007 aan een nationale transactiestandaard voor overheidsorganisaties, genaamde Digikoppeling. De huidige versie 2.0 is op onderdelen bruikbaar in het onderwijsveld en de aanstaande voor de overheid verplichte versie 3.0 voegt opties toe die in het onderwijs geschikt zijn.

Een directe aanleiding voor dit document is het project Digitaal Aanmelden. Hierbij wordt informatie uit externe bronnen bijeengebracht in een digitaal aanmeldingsformulier. Met name de complexiteit veroorzaakt door het gegeven dat een groot aantal scholen gebruik maken van een Leerling Administratie en/of Leerling Volg Systeem in de vorm van een cloudoplossing[1] maakt een sectorale afspraak noodzakelijk. Het gebruik van cloudoplossingen introduceert extra complexiteit, omdat technisch gegevens uitgewisseld worden met de cloudleverancier, terwijl inhoudelijk de gegevens bedoeld zijn voor of gevraagd worden van één van de scholen die gebruik maakt van die cloudoplossing. Momenteel werkt meer dan de helft van alle instellingen (per sector) met een cloudleverancier.

Tot nog toe kon dit probleem alleen opgelost worden door de technische identiteit van de onderwijsinstelling door een cloudleverancier te laten beheren. Dit betekent hoge administratieve lasten voor de onderwijsinstelling en hoge beheerlasten voor de cloudleverancier. Daarnaast bestaat er een zekere mate van schijnveiligheid omdat er niet rechtstreeks met de onderwijsinstelling zelf wordt uitgewisseld. Deze transactiestandaard lost dat op door de technische en inhoudelijke identiteiten van berichten te scheiden, waardoor gegevensuitwisselingen

[1] Zulke cloudoplossingen worden ook wel aangeduid als SAAS (software as a service).

door alle partijen (zowel cloud als niet-cloud) op een uniforme manier kunnen worden uitgevoerd.

§ 1.2 Inhoud

De Edukoppeling transactiestandaard beschrijft hoe de gestructureerde elektronische informatie-uitwisseling in het onderwijs is ingericht. Dit document geeft richtlijnen waarmee onderwijsinstellingen, uitvoeringsorganisaties en andere ketenpartijen eenvoudiger nieuwe gegevensuitwisselingen kunnen opzetten. Er worden allerlei aspecten rondom webservices en berichtenverkeer behandeld. De standaard dient gebruikt te worden bij alle projecten waarbij gegevensuitwisseling tussen verschillende partijen plaats gaat vinden. Dit document dient ook als naslagwerk in het geval van incidenten en problemen bij bestaande elektronische uitwisselingen en is bedoeld voor technisch georiënteerde architecten, technisch ontwerpers, programmeurs en applicatiebeheerders.

Dit document biedt ***toepassing-onafhankelijke*** richtlijnen. Edukoppeling richt zich op de ***koppelvlakken*** tussen de applicaties van de verschillende partijen en gaat uit van een ***contract-first*** benadering: bij een nieuwe informatie-uitwisseling worden de koppelvlakspecificaties eerst afgesproken en vastgelegd. Vervolgens zijn de partijen zelf verantwoordelijk voor hoe zij een applicatie ontwerpen. Het platform en de ontwikkelomgeving voor de applicatie is voor iedere partij vrij te kiezen, als het uiteindelijke berichtenverkeer tenminste maar aan de afgesproken koppelvlakspecificaties voldoet.

§ 1.3 Afspraken

In dit document is een aantal afspraken expliciet geformuleerd. Deze afspraken omvatten keuzes die de richting bepalen bij het inrichten van organisatieoverstijgende uitwisselingen. Op een rij:

Afspraak 01: Edukoppeling is de transactiestandaard voor servicegerichte gegevensuitwisseling in het onderwijs waarbij end-to-end security nodig is
Afspraak 02: Edukoppeling conformeert zich aan de Digikoppeling-standaard
Afspraak 03: Edukoppeling is **niet** gebaseerd op de Digikoppeling-EbMS
Afspraak 04: End-to-end security is uitgangspunt van Edukoppeling.
Afspraak 05: Verantwoordelijke beheert beveiligingsattribuut zelf
Afspraak 06: Edukoppeling sluit aan bij de OIN/HRN - systematiek
Afspraak 07: De service provider neemt autorisatiemaatregelen tegen ongeoorloofd gebruik

Afspraak 08: Edukoppeling geeft de OIN/HRN 's van de zendende en/of ontvangende partij door met WS-addressing

In de volgende hoofdstukken worden deze afspraken verder uitgewerkt en toegelicht.

§ 1.4 Doorvoeren van Edukoppeling

De Edukoppeling transactiestandaard vormt een onderdeel van een stelsel van afspraken, standaarden en voorzieningen (zie bijlage A) dat ketenpartijen in het onderwijsdomein in staat stelt op een eenduidige manier gegevens met elkaar uit te wisselen. Met de introductie van Edukoppeling wordt de logistiek rondom berichtenverkeer in het onderwijsdomein eenduidig gespecificeerd.

Voorafgaand aan deze standaard is er in het onderwijs vooral ervaring opgebouwd met eenvoudige vraag-antwoord uitwisselingen. Deze standaard bouwt voort op die ervaring en introduceert meer mogelijkheden zoals reliable messaging en grote berichten.

Organisaties die conform Edukoppeling werken doen dat typisch met behulp van een communicatiesoftware die poort, gateway of adapter wordt genoemd. Om volgens deze standaard te kunnen werken zijn aanpassingen nodig op die communicatiesoftware. Vanuit de referentie architectuur (ROSA)[2] worden handreikingen gedaan als instructies, broncode of proefomgevingen, om de overgang voor individuele organisaties te vergemakkelijken.

§ 1.5 Historie

Versie	Auteur	Datum	Opmerking
0.5	Gerald Groot Roessink	19-09-2013	Goedgekeurd door BOP-Generiek DUO
0.92	Gerald Groot Roessink en Remco de Boer	27-09-2013	Afgestemd met cloudleveranciers in het PO, VO en MBO, OSO (Kennisnet), Studielink en Architectuurraad EduStandaard (versie 0.92)
0.93 / 1.0	Gerald Groot Roessink en Remco de	06-12-2013	Goedgekeurd door Kerngroep RAO en ingediend bij EduStandaard

[2] Implementatiedocument en eventueel andere handreikingen dienen nog opgesteld te worden (verwacht in 2014), zie ook: http://www.wikixl.nl/wiki/rosa/

	Boer		
1.1	Gerald Groot Roessink en Remco de Boer	06-03-2013	Wijzigingen verwerkt n.a.v. openbare consultatieronde.

Ten opzichte van versie 0.92 zijn de volgende onderdelen gewijzigd.
In een spreadsheet verzamelde reviewcommentaren zijn verwerkt. Deze is separaat beschikbaar. Enkele grote wijzigingen:

- De afspraken over bewerkersovereenkomst en goedkeuringsproces zijn weggehaald omdat inmiddels een traject voor certificering of kwalificering voor cloudleveranciers[3] op gang is gekomen.
- De OIN nummer systematiek is veranderd: niet meer BRIN volgnummers, maar administratieve eenheden zijn logistiek belangrijk. Vergt nog wel centraal beheer.
- Afspraak over niet gebruiken SOAP-attachments is verwijderd. Dat is staande praktijk binnen OSO.
- OIN in de SOAP header is veranderd in IdentificatieKenmerk
- In bijlage A zijn deze transactiestandaard en andere componenten van Edukoppeling weergegeven.

Ten opzichte van versie 0.93/1.0 zijn er vooral tekstuele aanpassingen doorgevoerd voor de leesbaarheid en kleine inhoudelijk onjuistheden of onvolledigheden met betrekking tot Digikoppeling. De grootste wijzigingen zijn:

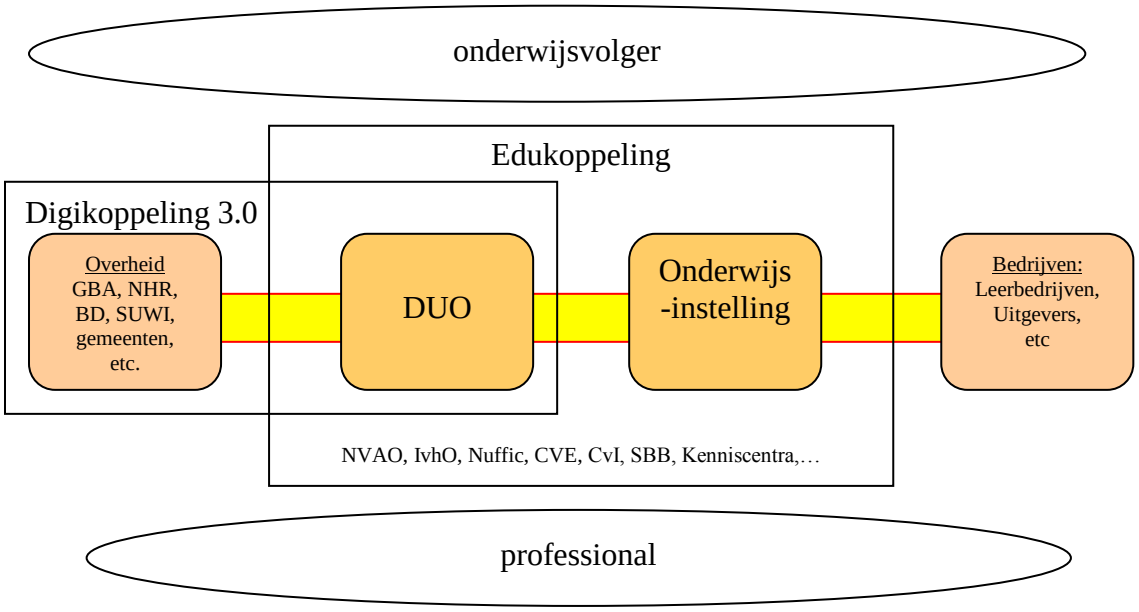
- De tekst van afspraak 01 is specifieker gemaakt, waardoor duidelijk wordt wat het toepassingsgebied is van de standaard.
- De vraag aan de Standaardisatieraad over de scope van de standaard (laatste alinea van de huidige par. 1.4, voorheen 1.3) is weggelaten.
- De opbouw van hoofdstuk 1 is veranderd:
  - De samenvatting is verwijderd i.v.m. overlap met par. 1.5. Historie (voorheen par. 1.4).
  - Deze paragraaf is - met uitzondering van versiegeschiedenis - verplaatst naar een nieuwe par. 1.1 Aanleiding.
  - En par. 1.3 uit de vorige versie (Verschillen met de vorige versies) is samengevoegd met de huidige par. 1.5 Historie.
- Voetnoot 1, 2, 3, 4, 9, 13, 14, 19, 21 en 22 zijn toegevoegd.
- De term SAAS-leverancier is veranderd in cloudleverancier.
- De term certificatieschema is veranderd in certificerings- of kwalificeringsschema. Dit schema (en de positionering er van) is nog in ontwikkeling.

[3] http://www.sionderwijs.nl/projecten/ref-arch-onderwijs/

- In tabel 1 is de kolomtitel Familie veranderd in Standaarden/profielen.
- De best practice op pagina 10 is aangevuld.
- Naast OIN ook HRN toegevoegd als identificatienummer voor private organisaties als onderdeel van het basisformaat zoals gehanteerd door Digikoppeling.
- Alinea op pagina 15 onder Afspraak 03 toegevoegd ter verduidelijking.
- Verbeteringen in tabel in bijlage B doorgevoerd.

Hoofdstuk 2 Positionering

In de onderwijsketen hebben we te maken met de systemen van de verschillende partijen die onderling service- en berichtenverkeer afspreken.



Figuur 1. Scope van Edukoppeling

Om niet iedereen het wiel opnieuw te laten uitvinden is er standaardisatie nodig. Standaarden geven houvast en enige zekerheid voor de toekomst. Dit hoofdstuk biedt een overzicht van de verschillende standaardisatie-initiatieven, en de relatie ervan tot de Edukoppeling Transactiestandaard.

§ 2.1 Internationale Standaarden

Als resultaat van gezamenlijke internationale samenwerkingsverbanden ontstaan er breed geaccepteerde internationale standaarden, ook op het gebied van gestructureerde gegevensuitwisseling. Sommige van die standaarden hebben inmiddels aanzienlijke draagkracht in de internationale gebruikersgemeenschap, en in de industrie die in bijbehorende software moet gaan voorzien.

Het is zinvol om waar mogelijk te conformeren aan internationale standaarden. Voorbeelden van belangrijke en relevante standaardisatieorganisaties: W3C en OASIS. Een in dit verband belangrijke standaard is WS-BRSP (voorheen WS-I) Basic Profile 1.1 van

OASIS[4], en de daarin gerefereerde W3C standaarden SOAP 1.1[5] en WSDL 1.1[6].

§ 2.2 Nationale Standaarden

De Nederlandse overheid heeft een standaardenbeleid dat wordt belichaamd door het College van Standaardisatie. Het college publiceert een zogenaamde pas-toe-of-leg-uit lijst met een verplichtende karakter voor de overheid.

In de volgende drie subparagrafen zijn relevante nationale standaarden opgenomen.

§ 2.2.1 Digikoppeling

De NORA[7] is de referentie architectuur van de Nederlandse overheid. Dit is service georiënteerde architectuur waardoor de inspanningen van de overheid inhoudelijk worden gecoördineerd in de richting van een servicebus. Digikoppeling vormt de technische invulling van de servicebus. Digikoppeling is gebaseerd op internationale standaarden en wordt nationaal afgestemd met de uitvoeringsorganisaties van de overheid en vertegenwoordigers van de softwareindustrie.

Digikoppeling[8] gebruikt onderdelen van verschillende standaardenfamilies voor verschillende uitwisselingspatronen.

Standaarden/ profielen	**Uitleg**	**Patroon**	**Status?**
WUS	WSDL, UDDI, SOAP	Request-response (synchroon)	Pas-toe-of-leg-uit
EbMS	EbXML	Betrouwbare melding	Pas-toe-of-leg-uit
GB	metabericht + http-get	Grote berichten	Pas-toe-of-leg-uit
WS-RM (uitbreiding WUS profiel)	WSDL, UDDI, SOAP	Betrouwbare melding + asynchroon	Digikoppeling 3.0 vastgesteld, opname op lijst 'pas toe of leg uit' volgt (naar

[4] Zie: http://www.ws-i.org/profiles/basicsecurityprofile-1.1.html
[5] Zie: http://www.w3.org/TR/2000/NOTE-SOAP-20000508/
[6] Zie: http://www.w3.org/TR/wsdl
[7] Zie: http://www.noraonline.nl/wiki/Hoofdpagina
[8] Zie: http://www.logius.nl/producten/gegevensuitwisseling/digikoppeling/

			verwachting in mei 2015.

Tabel 1. Digikoppeling-varianten

- Request-response (synchroon)

De WUS-variant wordt gebruikt voor synchrone uitwisseling. Typisch is dat het geval als vanuit een organisatie gegevens worden opgevraagd met een webservice. De duur van zo'n synchrone raadpleegsessie is beperkt. Bij een time-out worden geen maatregelen getroffen voor herstel van de verbinding.

- Betrouwbare melding en asynchroon

Het WUS-protocol is minder geschikt voor berichten waar de ontvanger iets mee moet doen (controleren, opslaan, o.i.d.). Een voorbeeld is de overdracht van een dossier of een abonnementsmelding. In dit soort gevallen moeten bij een timeout wél maatregelen worden getroffen tegen verlies. Dit is waarom Digikoppeling ook de variant met EbMS kent. Het bericht wordt gegarandeerd afgeleverd. WUS en EbMS zijn echter niet verwant. Een ketendeelnemer moet daarvoor verschillende technieken in huis halen.

Met ingang van Digikoppeling 3 kunnen ketendeelnemers binnen de WUS-familie van standaarden ook betrouwbare meldingen (reliable messaging) realiseren. Dit is gebaseerd op de toevoeging van WS-reliable messaging 1.1 aan de WUS-familie van standaarden. Reliable Messaging is opgebouwd uit een aantal functies waarmee op protocolniveau gegarandeerd kan worden dat berichten als bedoeld aankomen.

Functie	**Òmschrijving**
Aangetekend	Indien een bericht niet door de ontvanger wordt bevestigd door een niet beschikbare server-applicatie wordt het bericht na <instelbaar> opnieuw verzonden. Dat gebeurt maximaal een <instelbaar> aantal keren.
Op volgorde	Een reeks van berichten wordt uitsluitend afgeleverd in de volgorde waarin ze zijn aangeboden. Bij een afwijking wordt om herzending gevraagd.
Ontdubbeld	Elk aangeboden bericht wordt exact eenmaal afgeleverd bij de ontvangende partij. Een bericht dat dubbel wordt ontvangen wordt uitgefilterd.

Tabel 2. Aspecten van reliable messaging

Best practice: *beheer ketenproces*
Als een bericht een maximaal aantal retry's zonder succes is uitgevoerd moet dit anders worden opgelost. Het signaal dat het bericht niet kon worden verstuurd, moet daartoe worden opgepakt en afgehandeld. Door de ketenpartners wordt een actieplan afgesproken voor als dit zich voordoet. De uitvoering daarvan kan deels worden gedaan door een door een serviceorganisatie op ketenniveau. Een dergelijk platform krijgt ook vorm binnen de overheid.

De WS-RM variant ondersteunt ook asynchrone request-response. In tegenstelling tot een synchrone request-response kan de response geruime op zich laten wachten. Er wordt bij asynchroon verkeer twee keer een communicatiesessie opgezet. De tweede sessie verwijst naar message-id van het oorspronkelijke sessie.

- Grote Berichten

De basispatronen die hiervoor zijn beschreven, zijn in beginsel gericht op de afhandeling van individuele gevallen. Binnen Digikoppeling zijn daarnaast afspraken gemaakt over grotere berichten (>20 MB, of elke andere bilateraal afgesproken berichtomvang) waarbij de kans op storingen tijdens het transport groot is. De basis van deze afspraak is dat de verzender van een groot bericht een metabericht verzendt of ontvangt en de ontvanger het bericht van het aangegeven internetadres geautomatiseerd downloadt.

§ 2.2.2 Beveiligingsstandaarden en Digikoppeling

Digikoppeling wordt gebruikt voor het beveiligen van service- en berichtenverkeer van de overheid.

- Bescherming persoonsgegevens

De Wet Bescherming Persoonsgegeven (WBP) stelt eisen aan het verwerken van privacygevoelige gegevens. Relevant is het in de wet gemaakte onderscheid tussen verantwoordelijke en bewerker. De verantwoordelijke is degene die zelfstandig beslissingen neemt over een gegevensverwerking zoals een berekening, een uitwisseling of een schoningsactie. Tenzij daar vrijstelling voor is gegeven[9], meldt de verantwoordelijke het inrichten van de verwerking van privacygevoelige

[9] De wettelijke meldingsplicht voor verwerking van persoonsgegevens staat in de Wet bescherming persoonsgegevens (Wbp). Het Vrijstellingsbesluit Wbp regelt dat bepaalde gegevensverwerkingen van deze meldingsplicht zijn vrijgesteld. Zie ook de Handreiking Vrijstellingsbesluit Wbp van het CBP (https://www.cbpweb.nl/hvb/)

gegevens bij het CBP of een daartoe ingestelde functionaris voor gegevensbescherming (FG).

Er is een nieuwe Europese privacyverordening in de maak die naar verwachting in 2014 ingaat en die uit gaat van ketenaansprakelijkheid. Dat wil zeggen dat partijen die verantwoordelijk zijn voor de verwerking van privacygevoelige gegevens zich er van dienen te vergewissen dat er in de keten afdoende maatregelen zijn getroffen ter bescherming van de persoonsgegevens. De Europese verordening verandert de gebruikelijke houding waarbij elke organisatie alleen verantwoordelijk is voor zijn eigen stuk.

- Informatiebeveiliging

Voor informatiebeveiliging zijn de ISO-normen 27001[10] en 27002 opgesteld en op de pas-toe-of-leg-uit-lijst van het College Standaardisatie gezet. Hierbij wordt in brede zin gekeken naar beveiligingsaspecten als integriteit, beschikbaarheid, vertrouwelijkheid en onweerlegbaarheid.

Bij transport dient voorkomen te worden dat iemand vertrouwelijke gegevens kan inzien of beïnvloeden door berichten te onderscheppen of zich voor te doen als iemand anders. Concreet is dit door Logius voor Digikoppeling vertaald naar de eis dat het transport End-to-end[11] wordt beveiligd. Dit is gebaseerd op de mogelijkheden van WS-security 1.0. Binnen Digikoppeling, de WUS-familie, bestaan de volgende profielen.

Digikoppeling Wus-profielen	**Basis**	**Signing**	**Encryptie+Signing**
Best Effort	2W-BE	2W-BE-S	2W-BE-SE
Reliable Messaging	2W-R	2W-R-S	2W-R-SE

Tabel 3. WUS-mogelijkheden voor End-to-end security en Reliable messaging

End-to-end security is gebaseerd op:

1. basis
   In dit geval is er een rechtstreekse point-to-point (p2p) tussen twee schakels in de keten. Per definitie reikt een p2p-verbinding nooit verder. Basis is alleen bruikbaar voor end-to-end (e2e) als de

[10] Voorheen heette dit de Code voor Informatiebeveiliging.

[11] Zie Digikoppeling Identificatie en Authenticatie, versie 1.1. De endparty's komen overeen met de verantwoordelijken in de zin van de WBP.

communicatie direct tussen de ketenpartners plaats vindt of als tussenliggende partijen (bijv. cloudleveranciers) vertrouwd zijn.

2. encryptie
De inhoud van het bericht wordt versleuteld met de publieke sleutel van de ontvanger. De houder van de bijbehorende private sleutel kan het bericht ontsleutelen, anderen niet. Encryptie komt binnen Digikoppeling alleen voor in combinatie met signing.

3. signing
Een bericht wordt ondertekend met de private sleutel van de verzender. De ontvanger kan met de publieke sleutel onweerlegbaar controleren of de gegevens in ongewijzigde vorm afkomstig zijn van de verzender.

§ 2.2.3 Identificatie en authenticatie Digikoppeling

Het service- en berichtenverkeer van de overheid wordt beveiligd met behulp van PKI-certificaten.

Logius/PKI-overheid heeft zijn voorschriften geformuleerd voor de PKI-certificaten: PKI-overheidscertificaten[12] 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 zijn maximaal 3 jaar geldig. Logius heeft voor Digikoppeling binnen de PKI-overheidsfamilie aanvullende eisen afgesproken. We spreken daarom in dit document over PKI-Digikoppeling certificaten.

De certificaten worden uitgegeven door een aantal erkende CSP's[13]. De PKI-Digikoppeling certificaten zijn van het niveau STORK4. Bij de uitgifte hoort 'face-to-face' controle: de houder neemt het certificaat persoonlijk in ontvangst.

De CSP die het certificaat uitgeeft heeft de verantwoordelijkheid om de uniciteit van het subject (service) te waarborgen en te identiteit te vermelden in het certificaat in het veld Subject.serialNumber.
De unieke identificatie van overheidsorganisaties wordt Overheids Identificatie Nummer (OIN) genoemd; de unieke identificatie van private organisaties wordt Handels Register Nummer (HRN) genoemd. Het

[12] Zie http://www.logius.nl/producten/toegang/pkioverheid/
[13] Zie http://www.logius.nl/producten/toegang/pkioverheid/aansluiten/toegetreden-csps/

basisformaat van de OIN/HRN's[14] is: <prefix><nummer><suffix> van altijd 20 karakters.

Prefix	Code	Suffix
00000001	FIN Belastingdienst (9 pos)	"000"
00000002	FIN Belastingdienst (9 pos)	Volgnr. (3 pos)
00000003	KVK (8 pos)	Vestiging (4 pos)
00000004	Logius (9 pos)	Volgnr. (3 pos) of "000"

Tabel 4. OIN-systematiek Digikoppeling[14]

Het OIN/HRN wordt toegekend aan overheidsorganisaties en aan bedrijven. Het wordt door de CSP en/of de overheid (Logius) bepaald.

§ 2.3 Standaarden in de keten

De Referentie Onderwijs Sector Architectuur (ROSA)[15] is een servicegeoriënteerde architectuur voor de sector onderwijs. De ROSA is een afgeleide van de Nederlandse Overheids Referentie Architectuur (NORA), en heeft betrekking op een keten die ook de onderwijsinstellingen omvat[16].

§ 2.3.1 Edukoppeling

Edukoppeling heeft de topologie van een servicebus (zie begrippenlijst). Ketenpartners wisselen in beginsel zonder tussenkomst via het internet met elkaar uit of met een zelf gekozen bewerker uit.

Afspraak 01: Edukoppeling is de transactiestandaard voor servicegerichte gegevensuitwisseling in het onderwijs waarbij end-to-end security nodig is

Het aanbieden en afnemen van services op een servicebus tussen overheidsorganisaties is in detail uitgewerkt en verplicht gesteld door de Nederlandse overheid. Eén 'stopcontact' per ketenpartner maakt hergebruik mogelijk voor een veelheid van informatiestromen. Diezelfde overweging, een gemeenschappelijk elektronische snelweg of

[14] Zie: http://www.logius.nl/fileadmin/logius/product/digikoppeling/algemeen/Gebruik_en_Achtergrond_Digikoppeling_Certificaten_v1.2.1.pdf

[15] http://www.wikixl.nl/wiki/rosa/index.php/Hoofdpagina

[16] Het onderwijsveld heeft een eigen architectuur geformuleerd in het programma SION: de Referentie Architectuur Onderwijs. In 2014 wordt dit geconvergeerd met een nieuwe versie van de ROSA.

basisinfrastructuur, is ook gemaakt voor Edukoppeling. Hierdoor kan worden aangehaakt bij de al bestaande nationale afspraken en structuren.

Afspraak 02: Edukoppeling conformeert zich aan de Digikoppeling-standaard

Digikoppeling is beschreven in paragraaf 2.2.1. In de Edukoppeling transactiestandaard wordt dat als volgt toegepast:

- Raadpleging
  Voor synchroon verkeer, bijvoorbeeld er worden online gegevens uit een register opgehaald en in één sessie in een scherm geplaatst, wordt gebruik gemaakt van Digikoppeling-2W-BE profielen.

In bijlage B wordt geschetst hoe dit wordt ingericht bij Digitaal Aanmelden MBO waarbij de raadpleger rechtstreeks de burger is.

- Asynchroon verkeer
  Voor asynchroon verkeer waarbij de verwerking van de gegevens niet altijd direct plaats kan vinden, bijvoorbeeld er worden gegevens gemeld aan een register, wordt gebruik gemaakt van Digikoppeling-2W-R profielen. De verwerking van de gegevens kan niet altijd direct plaats vinden. In dit geval wordt er asynchroon een verbinding opgezet voor de terugmelding van het resultaat. De tweede sessie verwijst naar de eerste.

- Notificatie
  Voor het versturen van berichten zonder een terugmelding, bijvoorbeeld bij een abonnementsdienst, wordt gebruik gemaakt van Digikoppeling-2W-R profielen.

Afspraak 03: Edukoppeling is niet gebaseerd op de Digikoppeling EbMS

Sinds Digikoppeling 3.0 zijn er twee profielen voor het patroon 'betrouwbare aflevering': EbMS en WUS met WS-RM profiel. EbMS geldt hierbij als de minst ondersteunde en het wordt niet of nauwelijks gebruikt in het onderwijsveld.

Door één standaard (WUS) te hanteren is de verwachting dat er een hogere adoptiegraad ontstaat, dat er betere interfacingmogelijkheden worden geboden, en dat kennisdeling binnen het onderwijsveld wordt gestimuleerd.

- Groot verkeer
  Voor batchgewijze uitwisselingen, of de uitwisseling van grote samengestelde informatieproducten, wordt Digikoppeling-GB gebruikt.

Dit is de combinatie van een WUS-bevraging (pull) of WUS-melding (push) bericht en een https-opdracht om het in het metabericht opgegeven bestand op te halen.

Best practice: Poort/gateway/adapter

De beperking tot nationale profielen maakt het mogelijk om standaardoplossingen voor de uitwisseling te kiezen. Er zijn producten op de markt die Digikoppeling (en dus ook Edukoppeling) compliant kunnen uitwisselen.

§ 2.3.2 Beveiligingsstandaarden

Net als Digikoppeling geldt dat in Edukoppeling beveiligd verkeer plaats vindt, maar met een nieuwe uitdaging. In substantiële mate werken onderwijsinstellingen namelijk 'in de cloud' met een LAS/LVS uitgevoerd als Software as a Service (SAAS). Daarmee zal de onderwijsinstelling zijn verantwoordelijkheid voor bescherming persoonsgegevens en informatiebeveiliging 'op afstand' regelen. Dit heeft het voordeel dat de onderwijsinstelling hiervoor zelf geen specialistische kennis hoeft te hebben.

De verantwoordelijkheid blijft echter altijd bij de onderwijsinstelling liggen en de aandacht van bescherming persoonsgegevens en informatiebeveiliging verschuift naar het zeker stellen daarvan. Dat kunnen technische maatregelen betreffen die in deze transactiestandaard zijn beschreven, maar ook procedurele maatregelen als een certificerings- of kwalificeringsschema en bijbehorende bewerkersovereenkomst.

Naast deze standaard wordt daarom een certificerings- of kwalificeringsschema ontwikkeld met normen voor cloudleveranciers die conform de technische afspraken uit deze transactiestandaard gegevens wilen uitwisselen in de onderwijsketen. Met dit schema is het in het kader van Digitaal aanmelden in het MBO (Bijlage C) mogelijk gemaakt om op basis van 1 PKI-certificaat (ofwel de technische identiteit) van de cloudleverancier i.p.v. de onderwijsinstelling uit te wisselen met DUO. Dit schema is een aparte bouwsteen en maakt geen onderdeel uit van deze transactiestandaard.

§ 2.3.3 Identificatie en authenticatie

Vanuit beveiligingsoptiek geldt de eis dat een organisatie de identiteit van zijn ketenpartner vaststelt om er zeker van te zijn dat berichten bij de

goede organisatie aankomen of (ongeschonden) afkomstig zijn van een zekere organisatie.

Afspraak 04: End-to-end security is uitgangspunt van Edukoppeling.

Edukoppeling veronderstelt dat de verantwoordelijke (de onderwijsinstelling) verzender en ontvanger 'iets' (het attribuut) heeft op basis waarvan de ketenpartner de identiteit kan vast stellen. Dat attribuut moet passen bij de risicoklasse dat voor de uitwisseling geldt[17]. Mogelijke attributen:

- PKI-Digikoppelingcertificaten

  Dit zijn certificaten die worden uitgegeven in het kader van PKI-overheid van Logius. De certificaten worden uitgegeven door erkende CSP's.

Let op:
Niet alle PKI-overheidscertificaten zijn bruikbaar. Iemand die een PKI-overheidscertificaat bestelt bij een CSP moet expliciet aangeven dat deze voldoen aan de Digikoppeling-eisen, anders bestaat de kans dat de aanvrager een certificaat ontvangt zonder OIN/HRN.

- PKI-Onderwijscertificaten

  Dit zijn certificaten die vanaf 2014 door DUO worden verstrekt in het kader van een wettelijke uitvoeringsregeling. Deze certificaten zijn technisch vergelijkbaar met PKI-Digikoppeling[18]. Het beveiligingsniveau is mede gebaseerd op de bestaande bekostigingsrelatie tussen DUO en onderwijsinstelling.

De PKI-certificaten kunnen worden gebruikt voor signing en encryptie zoals in Digikoppeling. Hiermee is het principe van een 'soap-intermediair' mogelijk, die als een soort digitale postbode de envelop gesloten en de inhoud ongemoeid laat. Dat werkt niet voor een cloudleverancier die per definitie wel iets met de inhoud doet. Daarvoor moeten dus nadere (technische en organisatorische) afspraken worden gemaakt.

[17] DUO hanteert hierbij het uitgangspunt dat zodra er persoonsgerelateerde gegevens in het spel zijn dat een middel wordt gebruikt dat minimaal voldoet aan de eisen van STORK 3 (two-factor).
[18] Zie Certificate Protocol Statement (momenteel nog concept).

Afspraak 05. Verantwoordelijke beheert beveiligingsattribuut zelf

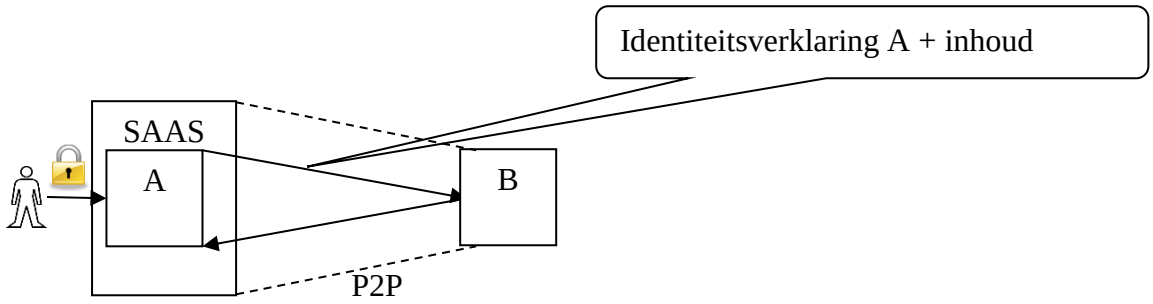
Om end-to-end security te realiseren in de situatie waarbij de instelling de bewerking overlaat aan een cloudleverancier wordt gebruik gemaakt van een digitaal toegangsattribuut.

Best practice:
In het onderwijs worden op grote schaal digitale toegangsattributen verstrekt aan leerlingen, leraren of administratief personeel. Er zijn twee federaties (Kennisnetfederatie, Surfconext) die dit, single-sign on, faciliteren. Het (stork) niveau van deze middelen hangt af van het type attribuut.

Een authenticatiedienst kan een zogenaamde identiteitsverklaring afgeven. Deze kan op twee manieren worden ingezet voor end-to-end security:

- in het verkeer

Indien een medewerker van requester A met een cloudoplossing direct of indirect de wil heeft geuit om berichtenverkeer te starten, dan kan de door de authenticatiedienst ondertekende identiteitsverklaring worden meegegeven met het bericht. Dergelijke oplossingen zijn bekend van RDW en Digipoort/E-herkenning. De responder B weet daarmee zeker dat een bericht afkomstig is van een zekere onderwijsinstelling.

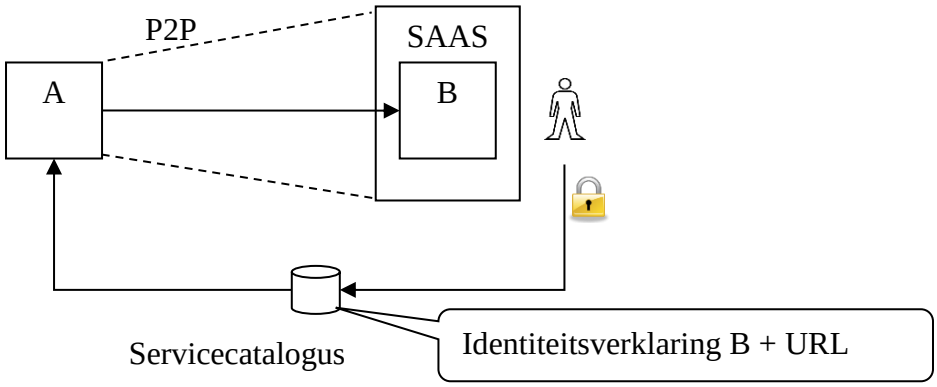


Best practice: Traffic Centre (TC)
Het TC van het Overstapdossier Onderwijs (OSO) heeft end-to-end security doordat het TC een sessie-id afgeeft voor een gevalideerde OSO-request. De sessie-id is gekoppeld aan de identiteit van de aanvragende school.

- vóór het verkeer

Als het daarentegen gewenst is dat de requester A de identiteit van de responder B met een cloudoplossing vaststelt, bijvoorbeeld bij

een notificatie van een verhuizing, dan gebeurt dat vooraf. De responder B laat een wilsuiting vastleggen in de beveiligde service-catalogus of 'gouden gids'. Dit houdt in dat de requester A wordt verzocht om de gegevens te leveren op een door de responder B bepaald URL of internetadres.



In beide situaties is met TLS een point-to-point (P2P)verbinding opgezet, zodat is gegarandeerd dat het verkeer tijdens het transport is versleuteld. Voor de versleuteling kan de verwerker – bijv. een cloudleverancier - een eigen PKI-certificaat[19] gebruiken.
Uit het beveiligingsattribuut (PKI-certificaat of identiteitsverklaring) kan afgeleid worden welke organisatie verantwoordelijk is voor de gegevens-verwerking.

Best practice: servicecatalogus DUO hanteert voor het eigen service- en berichtenverkeer een Routerings en Autorisatievoorziening (RAV) met daarin het URL/internet adres waar gegevens naar toe moeten worden gezonden. De onderwijsinstelling geeft bij DUO de URL van de cloudleverancier aan.

Afspraak 06: Edukoppeling sluit aan bij de OIN - systematiek

In het onderwijs zijn verschillende typen organisaties of onderdelen daarvan actief:

Prefix	**Code**	**Suffix**
00000001	FIN Belastingdienst (9 pos)	"000"
00000002	FIN Belastingdienst (9 pos)	Volgnr (3 pos)
00000003	KVK (8 pos)	Vestig.(4 pos)

[19] Hiervoor zijn wel aanvullende procedurele afspraken nodig zoals geborgd binnen een certificerings- of kwalificeringsprogramma (par. 2.3.2)

00000004	Logius (9 pos)	Volgnr (3 pos) of "000"
00000007	'000'+ BRIN (4 pos)	Administratienr.[20] (5 pos)

Tabel 5. OIN-systematiek Edukoppeling

De uitwisseling in het onderwijs wordt vaak uitgevoerd door de onderwijsinstelling of een zelfstandig opererend onderdeel ervan (de aanleverpunten). Deze staan niet in het NHR. Hiervoor wordt het register BRIN van DUO gebruikt als resource van identiteit. Deze worden toegevoegd aan de systematiek met een eigen prefix (00000007).

§ 2.3.4 Autorisatie

Edukoppeling ondersteunt identificatie (wie is de ketenpartner?) en authenticatie (hoe weten dat zeker?). Dit is beschreven in de vorige paragraaf. Service- en berichtenverkeer kan verder niet zonder autorisatie (mag die ketenpartner dit?). Er kunnen daarbij twee niveaus worden onderscheiden:

- service-autorisatie
  Per servicerequester is vastgelegd in welke rol hij acteert en per rol welke services aangeroepen mogen worden (role based access control). Voorbeeld: alleen VO-school mag de verzuim-service van DUO aanroepen.

- data-autorisatie
  Servicerequester hebben slechts toegang tot hun eigen een deel van de bevraagde gegevensverzameling; Voorbeeld: School met BRIN=23XY mag alleen gegevens van eigen leerlingen raadplegen.

Afspraak 07: De service provider neemt autorisatiemaatregelen tegen ongeoorloofd gebruik

Dit betekent dat de service provider over autorisatie-informatie moet kunnen beschikking op het moment dat er een service wordt aangeroepen. Deze informatie kan afkomstig zijn uit een servicecatalogus. Deze standaard geeft geen verdere richting aan autorisatie en het, eventueel centraal, beheren van autorisatie-informatie.

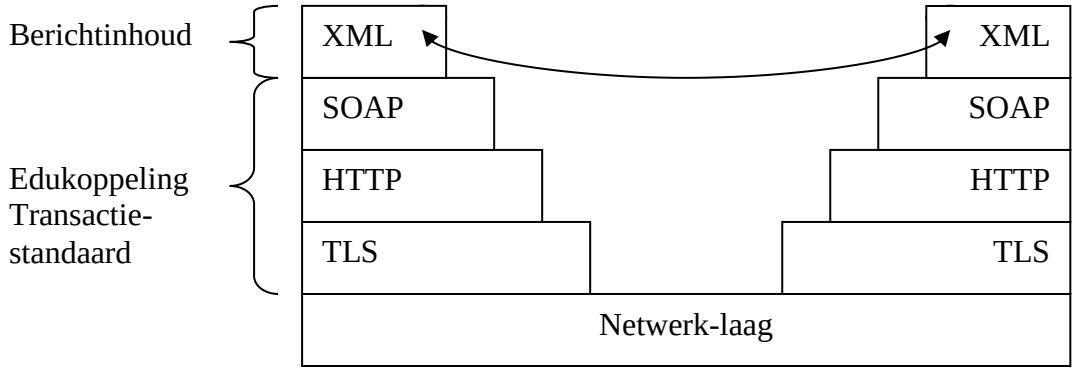
[20] Een onderwijsinstelling geïdentificeerd met BRIN (4pos) kan zijn administratie hebben opgesplitst. Dan kan samenvallen met de bekostigingsvestigingen in PO en VO, maar in principe is dat puur toeval. Die bekostigingsvestigingen hebben een functie bij de bekostiging en horen daarom in de payload. Voor de logistiek wordt daarom in OSO en door DUO ook gewerkt met 'aanleverpunten'. Helaas loopt dat door elkaar en klopt die naam niet meer vanwege de opkomst van SAAS. Daarom wordt hier uitgegaan van een nieuwe centraal verifieerbare registratie van administratiekantoren.

Hoofdstuk 3 Onderliggende technische basisstandaarden

Om tot gestructureerde informatie-uitwisseling tussen verschillende systemen te komen zijn er technische afspraken nodig op verschillende niveaus. Die afspraken worden vastgelegd in protocollen. In dit hoofdstuk beschrijven we de basisingrediënten.

§ 3.1 Verschillende Lagen

Het lagen-model uit Figuur 2 toont wat er gebeurt bij informatie-uitwisseling tussen twee partijen. Laag voor laag wordt bij de ene partij de boodschap steeds verder 'ingepakt' totdat het pakket klaar is om over de infrastructuur verzonden te worden. Bij de andere partij wordt het hele pakket dan weer laag voor laag uitgepakt totdat de originele boodschap overblijft.



Figuur 2. Lagen-model

De Edukoppeling Transactiestandaard beschrijft hoe de lagen 'SOAP', 'HTTP' en 'TLS' ingevuld dienen te worden. Voor het complete beeld worden hier alle lagen kort beschreven.

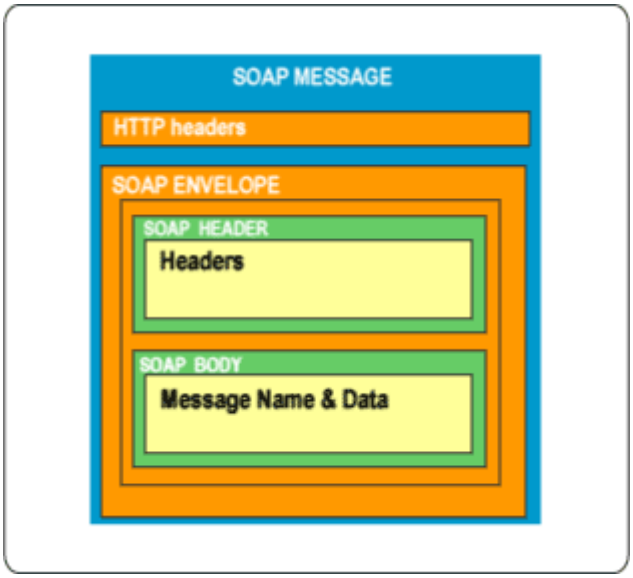
§ 3.2 De XML Laag

De bovenste laag is de XML laag, ook wel genoemd de 'Payload'. Op bedrijfs-applicatieniveau is bepaald dat er gegevens moeten worden uitgewisseld tussen verschillende applicaties / systemen. Hier is bekend welke gegevens uitgewisseld gaan worden en voor welke applicatie(s) de

gegevens bestemd zijn. De inhoudelijke functionele informatie die tussen partijen wordt uitgewisseld wordt vormgegeven en gestructureerd met behulp van XML. Over de betekenis en structuur van de berichten doet de Edukoppeling Transactiestandaard geen uitspraken.

§ 3.3 De SOAP Laag

De volgende laag is de SOAP laag. Hier wordt de inhoudelijke boodschap gestructureerd met XML, wordt voorzien van een 'envelop'. Digikoppeling refereert aan WS-BRSP (voorheen WS-I) Basic Profile 1.1 en andere WS-I profielen van OASIS, en de daarin gerefereerde W3C standaarden SOAP 1.1 en WSDL 1.1.



Figuur 3. Opbouw SOAP

De payload is opgenomen in de SOAP-body. Daarnaast kent SOAP minimaal één header en nul, één of meer attachments. Deze standaard schrijft voor hoe die ingevuld worden:

- SOAP-header

De SOAP-binding van webservices is in Digikoppeling gebaseerd op WS-addressing 1.0. Dit is gericht op het afleveren, routeren, identificeren en correleren van berichten.

Cloud Computing is een aandachtspunt bij SOAP-binding. Immers het moet mogelijk zijn dat de cloudleverancier aangeeft van welke onderwijsinstelling de gegevens afkomstig zijn en, andersom, de ketenpartner moet kunnen aangeven voor welke onderwijsinstelling de gegevens bestemd zijn.

Afspraak 8: Edukoppeling geeft de OIN's van de zendende en/of ontvangende partij door met WS-addressing

In onderstaande tabel is de SOAP-binding van webservices in Edukoppeling weergegeven. Aangegeven is hoe OIN's daarin zijn opgenomen.

Message Addressing Parameter (MAP)	MAP-Type	Message Exchange Pattern (MEP)			
		Request-synchroon	Response-synchroon	Request-asynchroon	Response-asynchroon (optioneel)
Wsa:To	URL	WSDL-Adres +OIN responder	'Anonymous' +OIN requester	WSDL-Adres +OIN responder	WSDL-Adres +OIN requester
Wsa:Action	URI	WSDL-Operatie	WSDL-Operatie	WSDL-Operatie	WSDL- Operatie
Wsa:MessageID	UUID	'eigen waarde'	-	'eigen waarde'	'eigen waarde'
Wsa:RelatesTo	UUID	-	Request: MessageID	-	Request: MessageID
Wsa:ReplyTo	EPR	'Anonymous' (optioneel)	-	-[21]	-
Wsa: From	EPR	'Anonymous' +OIN requester	'Anonymous' +OIN requester	'Anonymous' +OIN requester	'Anonymous' +OIN requester

Tabel 6. SOAP-binding in Edukoppeling.

Deze manier van werken komt overeen met de manier van werken van de vertaaldienst van Digikoppeling[22]. In tegenstelling tot Digikoppeling zijn alle OIN-aanduidingen in dit schema in Edukoppeling verplicht. Immers, zowel bij synchrone als bij asynchrone uitwisseling, zowel in de rol van requester en responder, speelt de OIN-aanduiding een rol bij cloudoplossingen.

Voorbeeld OIN in SOAP-header MEP request

```
<soapenv: Header>
    <wsa:To>
        http://www.intermediairx.nl/services          /* het WSDL-adres */
        ?oin=12345678901234567890 /* OIN responder */
    </wsa:To>
    <wsa:Action>
        ontvangenLeerlinginformatie_V2                /* de WSDL-operatie */
    </wsa:Action>
    <wsa:MessageID>
```

[21] In Digikoppeling-2W-R is het mogelijk om met de reply-to parameter dynamisch het retouradres op te geven in de request. Het blijkt aanzienlijk eenvoudiger om tweeweg verkeer te implementeren als twee keer eenweg verkeer. Vandaar dat de reply-tot parameter wordt uitgesloten in Edukoppeling.

[22] http://www.logius.nl/fileadmin/logius/product/digikoppeling/Digikoppeling_3_0_TranslatieSpecificatie_v1_0_.pdf

```
            550e8400-e29b-41d4-a716-446655440000      /* uniek bericht-id */
      </wsa:MessageID>
      <wsa:From><wsa:Address>
            http://www.w3.org/2005/08/addressing/anonymous   /* dummy */
            ?oin=98765432109876543210 /* OIN requester */
      </wsa:Address></wsa:From>
   </soapenv: Header>
```

- SOAP attachment

Sinds Digikoppeling 2 mogen attachments via MTOM/XOP (ook wel 'trailer elements') worden toegevoegd na de SOAP-body.

§ 3.4 De HTTP Laag

De HTTP laag verzorgt de bezorging van de berichten. Het SOAP bericht wordt naar een HTTP adres gestuurd. HTTP is de naam van het Transport protocol. HTTP informatie wordt meegestuurd met het bericht in de vorm van HTTP parameters. Dit is geheel standaard.

§ 3.5 De TLS Laag

Digikoppeling stelt point-to-point (p2p) security door middel van een TLS V1.0[23] met tweezijdige authenticatie op transportniveau (in het http-kanaal) verplicht. Hiermee wordt de http connectie versleuteld (het wordt een https-kanaal). TLS is een breed geaccepteerde en geïmplementeerde standaard daarvoor. Dit is de opvolger van, het als term bekendere, SSL.

Tweezijdig wil zeggen dat zowel de client als de server zich bekend maakt met behulp van een certificaat. Hiermee wordt het verkeer in beide richtingen versleuteld. Er is echter een beperking aan versleuteling op de TLS-laag: het reikt niet verder dan het eerste het beste knooppunt. End-to-end security kan daarom niet op de TLS laag worden gerealiseerd. Dat gebeurt alleen op de SOAP-laag.

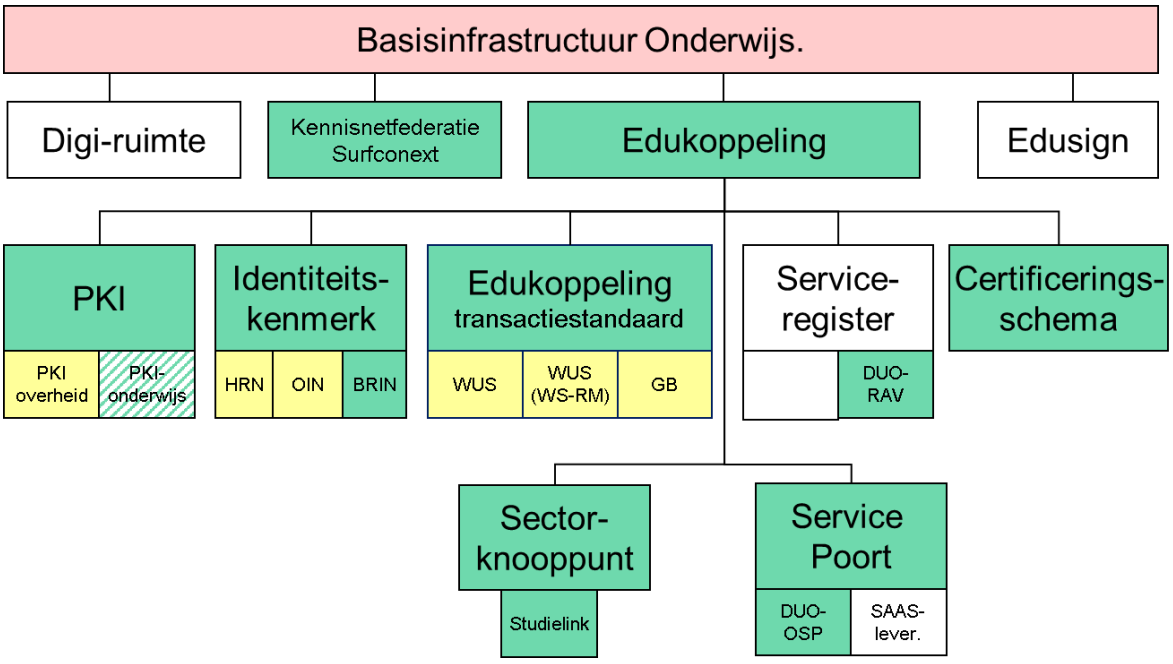
§ 3.6 De netwerklaag

Deze laag heeft betrekking op onder meer de fysieke verbindingen en het op het TCP/IP-protocol gebaseerde Internet. De Edukoppeling Transactiestandaard doet hier verder geen uitspraken over.

[23] Conform Digikoppeling, maar in strijd met het advies dat NCSC heeft gegeven. TLS 1.0 bevat kwetsbaarheden die in 1.2 verholpen zijn. Zie ook NCSC advies **Factsheet FS 2011-09.**

Bijlage A. Positionering Edukoppeling

De Edukoppeling transactiestandaard maakt onderdeel uit van de basisinfrastructuur van het onderwijs waarin ook actieve componenten zijn onderkend. Voor een deel zijn die gebaseerd op nationale voorzieningen en voor een deel zijn of worden die sectoraal ontwikkeld.



Figuur 4. Basisinfrastructuur onderwijs

De ROSA/RAO beschrijft uitgebreid de bouwstenen van de basisinfrastructuur onderwijs waartoe ook Edukoppeling behoort. Bij Edukoppeling rekenen we de Edukoppeling transactiestandaard (dit document) en de organisatorische of technische voorzieningen Certificeringsschema, PKI, OIN en Serviceregister.

Cruciale actieve componenten maken de toegang tot Edukoppeling mogelijk. Dit zijn de servicepoorten, gateways of adapters die door organisaties zelf (als bij DUO) of in de cloud (als SAAS) worden ingericht en sectorknooppunten (zoals Studielink) die een substructuur met eigen voorzieningen vormen. Organisaties kunnen samenwerken doordat Poorten en Knooppunten over serviceinformatie (wie biedt welke services waar aan en wie mag daar gebruik van maken) in het Serviceregister ter beschikking wordt gesteld.

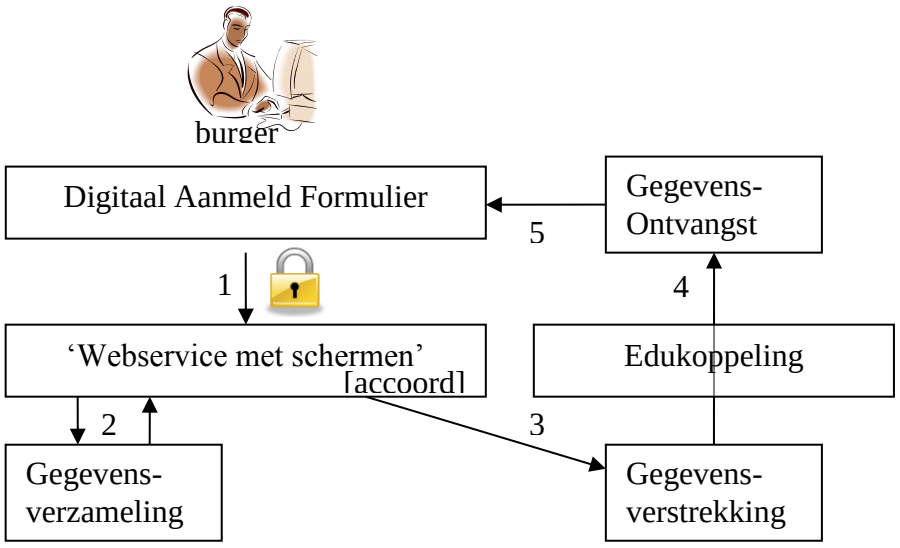
Bijlage B. Digikoppeling-Edukoppeling

Het schema laat ook zien dat de Edukoppeling transactiestandaard is gebaseerd op Digikoppeling. In dit document worden om pragmatische redenen aanvullende afspraken gemaakt specifiek voor het onderwijs. Dat is onder meer nodig omdat het onderwijsveld in veel gevallen in de cloud werkt en de overheid niet. Hierbij een samenvatting van de verschillen tussen Digikoppeling en de Edukoppeling.

Nr	Digikoppeling	Edukoppeling
1	SOAP-binding bevat alleen OIN/HRN's buiten de 'vertaaldienst' bij meldingen.	SOAP-binding bevat altijd OIN's vanwege routering achter de voordeur van de cloudleverancier
2	Meldingen met ebmS en WUS naast elkaar.	Geen EbMS. WUS gebaseerd op uitwerking DK3.
3	Reply-to toegestaan bij asynchroon verkeer.	Asynchroon verkeer geïmplementeerd als twee keer éénweg verkeer.
4	Beveiliging alleen op basis PKI-certificaten.	Beveiliging leunt op accreditatieprogramma en andere beveiligingsattributen.
5	Certificaten van het type PKI-overheid	Certificaten van het type PKI-overheid of PKI-onderwijs.
6	HRN/OIN's gebaseerd op NHR en Logius.	HRN/OIN-systematiekgebaseerd op NHR, Logius en BRIN.

Bijlage C. Digitaal aanmelden MBO

Niet in alle gevallen, maar in toenemende mate wordt het uitgangspunt dat de burger de regie heeft op de uitwisseling van 'zijn of haar' gegevens. Hierbij een schets hoe dat wordt ingericht bij Digitaal Aanmelden MBO en welke rol Edukoppeling daar bij speelt.



Figuur 4. Digitaal aanmelden MBO

Bijlage D. Bronnen

Documentnaam	Versie	Datum	Auteur(s)	Status
Strategische Informatiebeleidsplan 2013-2016	0.3	6 maart 2013	OCW/Directie Kennis	Concept
Architectuurschets van het stelsel voor gegegevensuitwisseling	1.0	24 mei 2013	W. Bakkeren, A. van Weel	Definitief
Koppelvlakstandaard WUS voor Digikoppeling 3.0	2.6.2	3 mei 2013	J. Li	Openbare consultatie
Koppelvlakstandaard ebMS: Digikoppeling 2.0	2.4	11 november 2012	Service Centrum Logius	Definitief
Digikoppeling_Koppelvlakstandaard_Grote_Berichten: Digikoppeling 2.0	1.1	5 april 2013	Service Centrum Logius	Definitief
Digikoppeling_Best_Practices_ebMS:_Digikoppeling 2.0	V1.5.2	11 november 2012	Service Centrum Logius	Definitief
Best Practice WUS Digikoppeling 3.0	1.4	24 maart 2013	J. Li	Concept
Digikoppeling Identificatie en Authenticatie	1.1	6 januari 2010	Logius	Definitief
Architectuur Digikoppeling 3.0	0.51	29 augustus 2013	Logius	Concept
Gebruik en achtergrond Digikoppeling certificaten	1.2.1	20 juni 2013	Logius	Definitief
MEMO Gegevensuitwisseling en multi-tenant SAAS	1.0	8 juli 2013	SION	Definitief
Whitepaper NCSC, cloudcomputing & security	1.0	01 januari 2012	NCSC	Definitie

Tabel 7: Brondocumenten

Bijlage E: Begrippenlijst

Onderwijsinstelling
De onderwijsgerelateerde organisatie die wordt geïdentificeerd met BRIN4.
Authenticatie
Het valideren van de identiteit van een organisatie die deelneemt aan Edukoppeling verkeer (‘ben jij wie je zegt dat je bent?’).
Authenticatiedienst
Een veelal sectorale of landelijke dienst gericht op het uitvoeren van authenticatie request van de service provider voor een organisatie die toegang probeert te krijgen. Voorbeelden zijn Kennisnetfederatie en Surfconext..
Autorisatie
Het bepalen of de service requester toestemming heeft voor de gevraagde dienst (‘mag jij wat je vraagt?’) of wat de het toegestane gegevensbereik voor de service requester is van de (‘waar mag je bij?’)
Aanleverpunt
Dit is een logistieke functie: iets of iemand die namens een onderwijsinstelling uitwisselt. Deze term verliest betekenis door de opkomst van cloudoplossingen (SAAS). Term niet meer gebruiken. DUO en Kennisnet (OSO) hanteren verschillende systematieken. Zie administratieve eenheid.
Administratieve eenheid
Dit is een administratieve functie: iets of iemand die namens een instellingen taken uitvoert. Dat kunnen er meer zijn per onderwijsinstellingen. Samenloop met vestigingen berust echter op toeval.
Bericht
Een bericht is onderling afgesproken formaat om gegevens uit te wisselen met een bepaald doel, soms ook wel bedrijfsdocument genoemd. De term kan ook betrekking hebben op een daadwerkelijk uitgewisselde instantie.
BRIN
Basisregister Instellingen. Register beheert door DUO met daarin alle bekostigde en aangewezen onderwijsinstellingen en gelieerde vestigingen. BRIN staat ook voor de identificatiecode van een instellingen van 4 posities.
Cloudleverancier
Leverancier van software 'in de cloud'. Zie ook SAAS.
Dienst
Een dienst is het resultaat of effect van een afgeronde inspanning waarmee in een behoefte van een burger of bedrijf wordt voorzien [NORA]. De termen 'dienst' en 'service' worden vaak door elkaar gebruikt.
Identificatie
Het relateren van een organisatie aan een registratie bij een identitititeitsprovider. In het onderwijs is dat in veel gevallen BRIN, maar ook het NHR en Logius worden gebruikt.
EbMS
Electronic Business Message Specification. Een standaard gedefinieerd door OASIS en toegepast binnen Digikoppeling. Niet gebruikt in Edukoppeling.
Edukoppeling
Deze standaard.

Encryptie
Een cryptografische techniek bedoeld om de vertrouwelijkheid van een boodschap te waarborgen. Bij Edukoppeling wordt gebruik gemaakt van asymetrische encryptie met een publieke en een private sleutel.
GB
De grote berichten variant van Digikoppeling. Wordt ook toegepast in Edukoppeling.
NORA
De Nederlandse Overheid Referentie Architectuur bevat inrichtingsprincipes, modellen en standaarden voor het ontwerp en de inrichting van de elektronische overheid.
Digikoppeling
Digikoppeling faciliteert gegevensuitwisselingen tussen overheidsorganisaties door standaardisatie van koppelvlakken (een overeengekomen set middelen en afspraken).
CSP of Certificate Service Provider
De uitgever van een PKI-certificaat. De uitgifte is gebonden aan stringente voorwaarden die zijn vermeld in een Certificate Protocol Statement (CPS). Op basis van de master key van de uitgever kunnen gebruikers het vertrouwensniveau bepalen. De uitgever houdt ook een Certificate Revocation List (CRL) bij zodat gebruikers kunnen checken of certificaten nog geldig zijn.
LAS/LVS
Leerling Administratie Systeem of Leerling Volg Systeem. Dit zijn applicaties van een onderwijsinstelling die veel gebruik maken van Edukoppeling. Vaak uitgevoerd als Software as a Service (SAAS).
Melding
Hetzelfde als een notificatie. Vaak gecombineerd als gegarandeerde melding.
PKI
Public Key Infrastructure. Geheel van processen en systemen gericht op het uitgeven van PKI-certificaten.
OIN
Overheids Identificatie Nummer. Dit is het nummer dat wordt gebruikt op een deelnemer van Digikoppeling en Edukoppeling uniek te identificeren. Wordt opgenomen in het PKI-certificaat.
Raadpleging
Een raadpleging is een transactie waarbij request en response in een enkele synchrone sessie worden uitgevoerd.
Request
Een verzoekbericht om een service te verlenen. Dat kan zijn een verzoek om gegevens te leveren (bij een raadpleging), maar let op: het kan ook een verzoek zijn om gegevens te accepteren (bij een notificatie).
Response
Het antwoordbericht op een request. Afhankelijk van het gekozen uitwisselingspatroon kan de respons synchroon, asynchroon of afwezig zijn.
Notificatie
Enkelvoudig bericht waarbij op de request geen response volgt. Dient voor het verstrekken van gegevens én gevalsoverdracht zodat procesuitvoering bij de andere partij verdergaat. Vandaar reliable dwz gegarandeerd uitgevoerd.
RAO
Referentie Architectuur Ondewijs. Is onderwijssector overstijgende architectuur van het ondewijsveld. Gaat mogelijk gecombineerd worden met ROSA.

ROSA
Referentie Onderwijssector Architectuur. Is de verbijzondering van de NORA voor de sector onderwijs. Gaat gecombineerd worden met RAO.
RM
Reliable Messaging. Methode om te zorgen dat berichten gegarandeerd aankomen, in de goede volgorde en maximaal eenmaal. Wordt gedefinieerd door W3C in de standaard WS-RM.
SOAP
Simple Objecty Access Protocol ook wel omschreven als de 'envelop' van een bericht. Bestaat uit header, body en attachment.
SAAS
Software as a Service. Is een vorm van Cloud Computing. Veel toegepast in het onderwijs. De leerling, leraar of administratief personeel logt remote in op het systeem van de cloud- of SAAS-leverancier.
Service: Een service is een geautomatiseerde (gegevens-)dienst die een organisatie aan andere organisaties aanbiedt. Een service voldoet aan een van de Digikoppeling koppelvlak specificaties en kan door een ander systeem worden aangeroepen.
Service aanbieder
Een partij die een webservice ter beschikking stelt, of een locatie op het netwerk waar berichten ontvangen en verwerkt worden. De partij zelf, is contextueel synoniem aan de webservice implementatie. [NORA: Serviceaanbieder]
Service afnemer
Een partij die gebruik maakt van webservice in de rol van afnemer, ofwel een bericht naar de webservice kan sturen. De partij zelf is contextueel synoniem aan de implementatie van de webservice client applicatie.[NORA: Serviceafnemer]
Servicebus
Een servicebus is een integratie-infrastructuur (middleware) die nodig is om een SGA (of SOA) te faciliteren. Zo ondersteunt de servicebus de webservices.
[NORA]: 'Servicebussen worden vanwege de genoemde eigenschappen steeds meer toegepast binnen afzonderlijke organisaties, maar ook binnen sectoren, landen en zelfs binnen de Europese Unie. Hierbij ontstaat dan een hiërarchisch stelsel van servicebussen, mede gebaseerd op het subsidiariteitsprincipe: binnen domeinen (organisatie, sector, e.d.) zijn partijen redelijk vrij in het maken van keuzes inzake de vormgeving en werking van de servicebus.'
Service provider
Zie onder 'service aanbieder' – beide termen worden door elkaar gebruikt.
Service requester
Zie onder 'service afnemer' - beide termen worden door elkaar gebruikt.
Serviceregister
Dit is een voorziening voor het beheer van serviceinformatie: wie biedt welke service waar (URL) aan en wie mag daar gebruik van maken? Deze informatie wordt gedistribueerd zodat ketenpartners kunnen autoriseren en routeren. Wordt ook wel Gouden Gids genoemd.
Signing
Signing is het plaatsen van een digitale handtekening onder een bericht. Dit gebeurt veelal door het bericht te 'hashen' met de private sleutel. Anderen weten dan zeker dat het bericht ongewijzigd is, afkomstig is van de verzender en de verzender kan niet ontkennen het aangemaakt te hebben.

Stork
Europese classificatie van beveiligingsniveau's. Zie http://www.forumstandaardisatie.nl/fileadmin/os/publicaties/Handreiking_Betrouwbaarheidsniveaus_def_tesktversie.pdf
SSL
Secure Socket Layer. Is een soort privé tunnel twee organisaties. Berichten worden daardoor geëncrypt. De term SSL komt nog voor maar is technisch vervangen door TLS.
TLS
Transport Layer Security. Is een soort privé tunnel twee organisaties. Berichten worden daardoor geëncrypt. Vervangt SSL.
Transactie
Een machinale uitwisseling tussen twee organisaties.
URL
Uniform Resource Locator. Dit is een uniek identificeerbare internetresource die concreet aanwijsbaar is (het is een internetadres).
Vertaaldienst
Een dienst die vertaalt tussen verschillende communicatieprotocollen, bijvoorbeeld tussen EbMS en WS-RM. Is gedefinieerd in Edukoppeling. Voor zover er andere protocollen worden gebruikt in het onderwijs wordt er vanuit gegaan dat daar de verantwoordelijkheid voor vertaling ligt.
Vestiging
Dit is een onderdeel van een onderwijsinstelling waarop in PO en VO een licentie berust en waarop leerlingen worden geteld. Dan kan maar hoeft zeker niet overeen te komen met een administratieve eenheid. Vestingen komen niet voor in Edukoppeling.
Webservice
Een webservice is een verbijzondering van een service waarbij het alleen services betreft die zijn gerealiseerd op basis van de W3C webservice specificatie (in de breedste zin van het woord, niet beperkt tot WS-*). De termen webservice en service worden als synoniemen gebruikt.
WSDL
Webservice Definition Language. Dit is het 'contract' tussen twee ketenpartners die met elkaar uitwisselen.
WUS
WSDL/UDDI/SOAP stack. Het is een stelsel uit de W3C WS-* standaarden

Bijlage F. FAQ

1. Kan de huidige situatie (implementatie PKI-certifcaat per instelling) blijven bestaan?
Voor bestaande gegevensuitwisseling kan, ook na de invoering van Edukoppeling, gebruik gemaakt blijven worden van de huidige technische voorzieningen. Dat betekent dat cloudoplossingen die nu werken met een PKI-certificaat per instelling dat kunnen blijven doen. Zodra er sprake is van een nieuwe situatie, wordt van scholen en leveranciers verwacht dat zij aansluiten bij de Edukoppeling-afspraken. Voorbeelden van zo'n nieuwe situatie zijn het aansluiten op een nieuwe dienst (service), het inrichten van een nieuwe vorm van gegevensuitwisseling.
Leveranciers die een certificate store hebben voor het beheren van het instellings-certificaten kunnen dat blijven doen als deze verlopen (normaliter na 3 jaar). DUO zal onderwijsinstellingen zonodig van nieuwe certificaten blijven voorzien. Edukoppeling omarmt wel de mogelijkheid om over te stappen op een certificaat per cloudleverancier. Daarvoor zijn enkele veranderingen noodzakelijk zoals een aangepaste berichtheader een identiteitsverklaring. In afstemming met de leveranciers zullen die veranderingen worden ingebracht in een nieuwe versie van bestaande gegevensuitwisselingen.

2. Hoe verhoudt een accreditatie zich tot de huidige kwalificering van bijvoorbeeld OSO of accreditatie van Studielink?
Kwalificering en accreditatie voor OSO en Studielink is gericht op deelname in een specifiek ketenproces: overdracht van studie- en begeleidingsgegevens (OSO) en aanmelden in het hoger onderwijs (Studielink). Het accreditatieprogramma van Edukoppeling is niet gericht op een specifiek ketenproces, maar heeft als voornaamste doel de positie van cloudleveranciers als partij bij gegevensuitwisseling in het onderwijs te formaliseren en end-to-end security te waarborgen. Onder end-to-end security verstaan we hier, zekerheid de cloudleverancier altijd en alleen handelt in opdracht van de onderwijsinstelling. Het maakt daarbij niet uit ten behoeve van welk ketenproces gegevens worden uitgewisseld.

3. Waarom voldoet het huidige uitwisselpatroon in de toekomst niet meer?
Steeds meer gegevens in het onderwijsdomein worden digitaal uitgewisseld. De eerste uitwisselingen waren van een betrekkelijk eenvoudige vorm: men stelde een vraag en kreeg een antwoord. Veel processen vragen echter om geavanceerdere vormen van gegevensuitwisseling. Zo kan het nodig zijn om gedurende bepaalde tijd een 'abonnement' af te sluiten op bepaalde gegevens, bijvoorbeeld om als school steeds de meest recente gegevens over een (aankomend) leerling te hebben. Ook kan een proces vereisen dat gegevens asynchroon worden uitgewisseld, bijvoorbeeld omdat de aanvraag van bepaalde gegevens eerst door een medewerker van de school moet worden beoordeeld, of omdat bepaalde gegevens eerst moeten worden klaargezet. En een veel gehoorde wens is dat het handmatig up- en downloaden van batchbestanden in bestaande uitwisselingen geautomatiseerd wordt. In al deze uitwisselpatronen voorziet Edukoppeling.

4. Wat is het voordeel van Edukoppeling voor mijn school?
U kunt Edukoppeling zien als een standaard stopcontact op de informatie-infrastructuur, bruikbaar voor een veelheid van toepassingen binnen het onderwijsveld en met de overheid. Edukoppeling vervangt niet bestaande ‘stopcontacten’, maar beoogt die te combineren. U

merkt er als school weinig tot niets van, anders dan dat nieuwe uitwisselingen sneller tot stand komen.

Het certificerings- of kwalificeringsprogramma voor cloudleveranciers en de Edukoppeling standaard geven u als school zekerheid dat de leverancier voldoet aan meest gangbare eisen van informatiebeveiliging en bescherming persoonsgegevens. Ook maakt Edukoppeling het mogelijk om dat de procedure voor PKI-certificaten per instelling wordt vervangen door een PKI-certificaat per cloudleverancier/bewerker terwijl u toch praktisch en in formele zin aan het roer blijft staan van de gegevensverwerking met authenticatiediensten als Kennisnetfederatie/Surfconext. De relatie tussen uw school en de cloudleverancier legt u vast in een serviceregister, waardoor voor anderen steeds duidelijk is bij welke leverancier zij moeten zijn om met u gegevens uit te wisselen.

5. Wat is het voordeel van Edukoppeling voor mij als cloudleverancier?
Als cloudleverancier maakt u gebruik van economies of scale, en bedient u uw klanten zo veel mogelijk vanuit een gedeelde omgeving. Wanneer er vanuit uw cloudoplossing gegevens worden uitgewisseld, doet u dat echter uit naam van de klant. In de huidige situatie moet u zich daarbij letterlijk voordoen als die klant, door gebruik te maken van het voor die klant uitgegeven certificaat. Dat betekent dat u een certificate store moet inrichten waarin de certificaten van al uw klanten liggen opgeslagen, en dat bij gegevensuitwisseling steeds het juiste certificaat moet worden geselecteerd. Dat brengt een onnodige beheerlast voor uw organisatie met zich mee. Bovendien zijn er technische beperkingen aan deze manier van werken, die maken dat u niet aan kunt sluiten op nieuwe uitwisselpatronen zoals gegevensabonnementen. Door aan te sluiten bij Edukoppeling wordt u als cloudleverancier zelf erkend als partij in de onderwijsketen, waardoor u voor gegevensuitwisseling voor al uw klanten kunt volstaan met één certificaat voor uw eigen organisatie. Bovendien bent u voorbereid op nieuwe vormen van gegevensuitwisseling die de komende jaren steeds meer gebruikt zullen worden.

6. Hoe te beginnen met het toepassen van Edukoppeling?
In dit document en in de opgenomen verwijzingen zijn afspraken geformuleerd hoe berichten en dialogen tussen organisaties zijn opgebouwd. In het algemeen gesproken richt elke deelnemende organisatie een poort, gateway of adapter in of laat dat in richten, die het verkeer volgens Edukoppeling verzorgt. Dat gebeurt in nu in de praktijk voor het WUS-protocol ook, vaak geïntegreerd met het LAS/LVS. Voor Edukoppeling-WUS is bedoeld om eenheid te creëren in de SOAP-binding. Dat ligt iets anders met WS-RM of het GB-protocol. Deze worden nog niet toegepast maar zijn opgenomen in de standaard vanwege de gunstige gebruiksmogelijkheden. Er zijn al producten op de markt die hier mee om kunnen gaan, maar het is ook mogelijk dat een LAS-leverancier dit zelf ontwikkelt. Om te voorkomen dat dit pas gaat spelen als de vraag zich manifesteert, kan worden overwogen om handreikingen te ontwikkelen naar LAS-leveranciers als open source en testomgevingen.