Concept Verslag ES werkgroep Edukoppeling transactiestandaard

Aanwezig: Herrie Abbink (Educus), Robert Kars (DUO), Gerald Groot Roessink (DUO), Brian Dommisse (Kennisnet, voorzitter), Erwin Reinhoud (Kennisnet/Bureau Edustandaard).

Afwezig: Edwin Verwoerd (Iddink, VDOD), Peter Dam (Cito), Marc Fleischeuers (Kennisnet, BPV/Vroegtijdig aanmelden MBO)

Agendalid: Ernst-Jan van Heuseveldt (Rovict, VDOD)

Datum en locatie
4 juli 2018, 10:00-13.00 uur, Seats2Meet, Amersfoort

Agenda

1. Opening, mededelingen, vaststellen agenda
    a. Terugkoppeling AR
    b. Terugkoppeling TO DK
2. Doornemen verslag en actielijst
3. Nieuwe release
    a. Concept release notes
    b. Open punten in issuelijst
    c. Overige wijzigingen in documentatie
4. Toelichting transactiestandaard Suwi keten
5. Rondvraag & sluiting

1. Opening, mededelingen, vaststellen agenda

Edwin Verwoerd, Peter Dam en Marc Fleischeuers hebben zich afgemeld.
Agenda wordt zonder wijzigingen vastgesteld.

1.1. Bespreking implementatieondersteuning Edukoppeling in Standaardisatieraad

Er wordt terugkoppeling gegeven over de bespreking van het memo ‘Memo implementatie-issues en -ondersteuning Edukoppeling’ in de Standaardisatieraad. Een belangrijk punt van aandacht is dat het niet een bepaalde partij is die het gebruik van Edukoppeling oplegt. Het is de Standaardisatieraad die de toepassing van bepaalde standaarden binnen het onderwijs vaststelt. In het geval van Edukoppeling speelt hier tevens de overweging welke gegevens er tussen partijen uitgewisseld worden. Beide partijen stellen op basis van een risicoanalyse vast of Edukoppeling toegepast moet worden.

De kern van het memo betreft de behoefte aan ondersteuning. Dit geldt in principe voor elke standaard, indien men vragen heeft over de standaard zelf of het gebruik ervan moet men ondersteund kunnen worden. Ten aanzien van de standaard zelf is dit nu al geregeld via de Edustandaard Werkgroep. Partijen die vragen hebben over de functies en werking van de standaard kunnen hier terecht. Een complexer vraagstuk is ondersteuning bij het gebruik. De complexiteit van het implementeren van Edukoppeling hangt namelijk deels af van het gebruikte platformen en andere factoren zoals de (interne) infrastructuur. Het is een punt van urgentie waarvoor een oplossing moet komen. Hoe hier invulling aan gegeven kan worden is de hoofdvraag. Er is in essentie behoefte aan een pool van experts die ervaring hebben met implementaties in verschillende omgevingen. Om de gebruikers van de standaard in contact te brengen met deze experts (organisaties) wordt gedacht aan het publiceren van een lijst met contactinformatie. Daarnaast wordt er gedacht aan een forum waarop vragen en antwoorden geplaatst kunnen worden. Als laatste wordt er voorgesteld om een overzicht te publiceren van ketens waar Edukoppeling toegepast worden. Deze zaken worden aan Edustandaard teruggekoppeld met de vraag of hier voorzieningen kunnen worden ingericht. (actiepunt #78).

1.2. Bespreking memo REST georiënteerde standaarden in Architectuurraad

Er wordt terugkoppeling gegeven over de bespreking van het memo 'MEMO-Onderzoekvoorstel-uitbreiding-Edukoppeling-met-REST-georiënteerde standaarden' in de Architectuurraad. De architectuurraad heeft besloten de werkgroep Edukoppeling de opdracht te geven de volgende twee vragen te beantwoorden:

1. Inventariseer de mogelijkheden ten aanzien van maatregelen op het vlak van betrouwbaarheid, integriteit en vertrouwelijkheid op het REST-protocol. Relateer deze aan de Digikoppeling profielen Best Effort, Signed, Encrypted of combinaties. Geef daarbij een indicatie waar in de wereld dit wordt toegepast.
2. Kies een raamwerk van betrouwbaarheidsniveaus voor het machine-machine verkeer voor de komende vijf jaar. Baseer dit bijvoorbeeld op het raamwerk dat wordt gebruikt bij E-herkenning. Plot de opties uit de eerste onderdeel op het raamwerk, evenals de huidige Edukoppeling-opties. Formuleer vervolgens voorstellen om er voor te zorgen dat de komende minimaal vijf jaar tenminste een wijze van berichtuitwisseling in het "veiligste spectrum" gehandhaafd blijft en beschrijf zo precies mogelijk één of meerdere toepassings-/werkingsgebieden voor "lichtere varianten".

De werkgroep Edukoppeling wordt verzocht in het vierde kwartaal van 2018 verslag uit te brengen. Brian geeft aan dat er geld bij Kennisnet voor Edustandaard beschikbaar komt om externe hulp hierbij in te schakelen, zodat we enerzijds de gevraagde doorlooptijd kunnen waarborgen en anderzijds we denken dat een blik van buitenaf (bijv. iemand die bekend is met de API-strategie) op dit onderwerp heel goed kan werken. Edustandaard zal derhalve een offerte-aanvraag doen in de markt.

1.3. Terugkoppeling Technisch Overleg Digikoppeling (TO DK)

Identificatie van voorzieningen

Er zijn binnen de onderwijssector situaties waar we diensten (softwarepakketten) van private partijen willen kunnen identificeren. Zo wordt ook bij OSO met een aanleverpunt gewerkt waarin ook een pakket/dienst onderscheiden kan worden. Logius geeft aan dat de suffix van het OIN van private partijen "0000" moet bevatten. Hiermee kan een private partij geen OIN gebruiken om binnen de organisatie diensten of afdelingen te identificeren. Verder kan een subOIN alleen door overheidsorganisaties toegepast worden. Bij het TO DK werd de vraag gesteld of er binnen andere sectoren use cases zijn waar private partijen een fijnmaziger identificatie nodig hebben dan de organisatie-identificatie in het Handelsregister. Er blijkt beperkt animo voor dit onderwerp, maar het punt wordt wel in de actielijst opgenomen. De Edukoppeling werkgroep heeft nog geen signalen vanuit ketens opgevangen dat het ontbreken van een dergelijk fijnmazige identificatie nu een knelpunt vormt. Zo heeft ook OSO nu een werkende oplossing. Wel wordt verwacht dat dit in de toekomst mogelijk een aandachtspunt gaat worden. Er wordt een issue (#29) geregistreerd om dit verder inhoudelijk te bespreken en de ontwikkelingen bij Digikoppeling te blijven volgen.

REST

Net als binnen het onderwijs is ook de overheid volop bezig met het ontwikkelen en toepassen van REST georiënteerde tandaarden. Digikoppeling volgt deze ontwikkelingen, maar zal deze niet zelf inhoudelijk ontwikkelen. De nadruk zal liggen op het duiden van toepassingsgebied en werkingsgebied van verschillende standaarden. Een externe partij gaat een onderzoek uitvoeren. De werkgroep ziet enerzijds dit als een mogelijke interessante aanvulling op het onderzoek dat Edustandaard gaat uitvoeren. Voor daar waar deze elkaar gaan overlappen is het interessant om te zien of dezelfde conclusies worden getrokken.

Voorstel om in Digikoppeling optioneel het OIN in WSA:To en WSA:From toe te staan

De RFC wordt verwerkt in de te ontwikkelen DK WUS versie 3.6. Waarschijnlijk begin najaar wordt deze versie gepubliceerd. Er is geen overkoepelende versie meer en documenten kunnen sneller aangepast worden.

TLS ciphers

Logius heeft nogmaals met NCSC overlegd. NCSC geeft aan dat de hun lijst een bredere toepassing heeft dan alleen S2S koppelingen (ook ciphers voor browsers). Er werd geadviseerd om een specifieke lijst voor S2S

verkeer op te stellen. Of dit wordt opgenomen in de NCSC lijst of dat er een aparte lijst bij Digikoppeling beveiligingsvoorschriften bijgehouden wordt is nu nog niet duidelijk. Aan het eind van het jaar komt NSSC met een nieuwe lijst. Er wordt aangegeven dat hierin in ieder geval ook TLS 1.3 ciphers opgenomen gaan worden. Welke ciphers uit de bestaande lijst verwijderd worden is nog niet duidelijk. Het TO gaat in het najaar de conceptversie bespreken en eventuele acties bepalen.

SOAP faultcode in Digikoppeling foutbericht
Net als in Edukoppeling wordt ook voor Digikoppeling een foutbericht beschreven. Het is nu niet duidelijk of het samenvoegen van een Digikoppeling foutcode met de SOAP faultcode in een SOAP Fault een probleem gaat opleveren als hiervoor de dot-notatie wordt toegepast. Hetzelfde mechanisme passen we ook bij Edukoppeling toe en hebben hiervoor nu issue #19 voor geregistreerd. Of Digikoppeling als scheidingsteken een koppelteken of dot-notitie gaat toepassen staat nog open. Logius heeft hierover een vraag uitstaan bij OASIS. Op basis van de terugkoppeling door OASIS zullen we besluiten of in de nieuwe versie van de transactiestandaard de dot-notatie gehandhaafd blijft.

Verplicht gebruik PKIoverheid certificaten
De vorige bijeenkomst van de Edukoppeling Werkgroep kwam bij de bespreking van agendapunt 4 naar voren dat er onduidelijkheid is of PKIoverheid certificaten voor zowel client als server bij TLS, ondertekening en versleuteling verplicht zijn. Bij het TO DK werd dit nog eens bevestigd[1]. Bij een PKIoverheid certificaat is er bij de CSP een proces ingericht dat de identiteit van private partij controleert in het handelsregister. Hiermee is de identiteit en indirect de authenticatie via het certificaat geregeld. Bij niet PKIo CSP's is dit niet geregeld en kent men ook het OIN waarschijnlijk niet en kunnen andere key usages (combi's) toegepast worden. Dit is een risico verhogende factor. Bij het toestaan van andere certificaten zullen er vele verschillende CRL's van CSP's geraadpleegd moeten worden. De werkgroep stelt dat Edukoppeling koppelvlakken ook voor TLS een PKIoverheid certificaat moeten toepassen. Deelnemers wordt gevraagd dit in de achterban te benadrukken.

2. Doornemen verslag en actielijst van 16 mei 2018

Er wordt voorgesteld om de beschrijving van issue #15 'Gebruik ODOC certificaten' in het verslag te wijzigen. Hierbij moet opgenomen worden dat in het verleden de ODOC certificaten wel gebruikt werden bij S2S koppelingen. Het voorstel wordt overgenomen en wordt verwerkt in de definitieve versie van het verslag.

Toelichting GB profiel (actiepunt #24)
Dit actiepunt blijft staan, DUO gaat wel navraag doen of het GB profiel toegepast wordt.

Onderzoeken problematiek met SOAP 1.1 (actiepunt #57)
Digikoppeling is ondertussen gestart met het onderzoek rond ondertekenen van berichten. Toepasbaarheid van SOAP 1.2 wordt mogelijk meegenomen in onderzoek ondertekenen, omdat SOAP 1.2 hierbij voordelen biedt t.a.v. interoperabiliteit en/of implementeerbaarheid (met name Microsoft platform).

Release notes nieuwe versie publiceren (actiepunt #71)
Op basis van de wijzigingen uit de issuelijst is er een voorlopige release notes document opgesteld. De werkgroep vindt dit een acceptabele vorm om gebruikers van Edukoppeling te informeren over de wijzigingen van de nieuwe versie. Het document zal op de Edustandaard site geplaatst worden. In het najaar zullen hier mogelijk nog wat nieuwe punten in opgenomen gaan worden. De voorlopige conceptversie van de documenten wordt in september met de leden gedeeld.

Onderzoek problematiek andere certs dan PKIo bij TLS kanaal (#73)
Kunnen we besluiten of we Digikoppeling blijven volgen of worden voor servers andere type certificaten dan PKIo toegestaan? Als dit mag wat zijn de consequenties hiervan? Zoals ook bij mededelingen al is besproken is de werkgroep van mening dat op dit punt de Digikoppeling standaard gevolgd moet worden. Actiepunt is afgehandeld.

[1] In de DK beveiligingsvoorschriften staat: "TLS001: Authenticatie is verplicht met TLS en PKIoverheid certificaten"

Navraag bij Logius of er voor TLS, ondertekenen en versleuteling PKIo certs verplicht zijn (#74)
Bij het vorig overleg is het verplicht gebruik van PKIoverheid certificaten ter discussie gekomen. Navraag bij Digikoppeling (zie mededelingen TO DK) geeft aan dat Digikoppeling ook voor TLS een PKIoverheid voor client en server verplicht is. Actiepunt is afgehandeld.

Onderzoeken welke ketens grote bestanden (of gegevens in bulk) uitwisselen (#75)
Bij DUO en CvTE wordt navraag gedaan. Actiepunt blijft open.

Onderzoeken PKI SAN en mogelijke alternatieven (#76)
Navraag heeft opgeleverd dat er geen interoperabiliteitsproblemen zijn bij het toepassen van SAN certificaten. Omdat ook voor de server PKIo certificaten vereist worden moeten we wel vaststellen of hierbij geen beperkingen gelden. PvE PKIo kent geen maximum aan FQDN in SAN, er wordt gesteld: “Bij server certificaten MOET dit veld minimaal 1 FQDN bevatten.” CSP’s kunnen echter mogelijk wel een maximum hanteren (KPN stelt het maximum op 10). Het toepassen van een PKI(overheid) SAN certificaat zal worden beschreven (zie issue 21). Verder wordt wel met het SaaS model beoogd dat men in ketens (naar externe partijen) één Edukoppeling koppelvlak inricht. Hiermee is het ook niet meer noodzakelijk om SAN certificaten toe te passen. Actiepunt is afgehandeld.

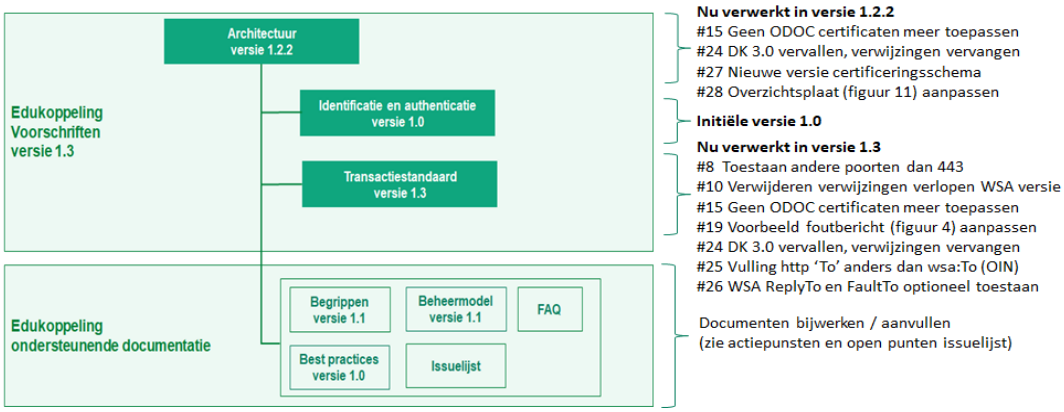
Documenteren van push en pull variant (#77)
Wordt opgenomen in de best practices. Actiepunt blijft open.

3. Nieuwe release

3.1. Concept release notes

We hebben eerder besloten dat we de wijzigingen van de nieuwe release op korte termijn willen publiceren zodat gebruikers hierover vroegtijdig geïnformeerd zijn. De werkgroep stemt in met de voorgestelde wijzigingen in de concept release notes en stelt dat deze voldoende informatie bevat. Er wordt wel aan de leden gevraagd om deze nieuwe release extra onder de aandacht te brengen in de verschillende ketens (actiepunt #79). De concept release notes zullen op de Edustandaard site gepubliceerd worden. Een kanttekening hierbij is wel dat we verwachten dat in het najaar nog wat wijzigingen volgen die we in de nieuwe release zullen opnemen. De uiteindelijke release notes die meegeleverd wordt met de nieuwe versie zal alle wijzigingen bevatten.

Met de komst van het Identificatie en Authenticatie document bestaat de Edukoppeling standaard nu uit drie documenten (zie ook Figuur 1). Tot op heden hadden de Architectuur en de Transactiestandaard dezelfde versie. In de nieuwe release zijn de wijzigingen in de Architectuur minor (versie 1.2.2) en in de Transactiestandaard medior (versie 1.3) van aard. Het I&A is een eerste definitieve versie 1.0. De documenten hebben nu dus elk een eigen versie. Hiermee ontstaat het vraagstuk hoe het beste over deze nieuwe release gecommuniceerd kan worden. Ketens willen graag afspraken kunnen maken over het implementeren van een specifieke versie, het verwijzen naar drie verschillende documenten is dan niet handig. Na bespreking van wat alternatieven wordt er besloten om in de release notes een overkoepelende versie-aanduiding op te nemen (versie 1.3). Hiermee hebben gebruikers inzicht in hoe deze nieuwe versie zich verhoudt tot de vorige en kunnen ketens duidelijk communiceren welke versie toegepast wordt. Wat de daadwerkelijk impact van de nieuwe versie is wordt beschreven in de release notes. Daarnaast wordt ook in de documenten zelf aangegeven wat er t.o.v. de vorige versie gewijzigd is. De wijzigingen in de ondersteunende documenten worden niet meegenomen in de release notes. Deze documenten vormen geen formeel onderdeel van de standaard afspraken en kunnen los van de standaard doorontwikkeld worden. Figuur 1 geeft een overzicht weer van alle documenten en de nieuwe versie.



Figuur 1 - Overzicht Edukoppeling versie 1.3

3.2. Open punten in issuelijst

Issue 5 (OPEN): Interoperabiliteit probleem bij ondertekenen. We verwachten aanscherpingen in september na afronding onderzoek. Afhankelijk van de resultaten van het onderzoek en of deze tijdig bekend zijn wordt dit mogelijk meenemen in versie 1.3.

Issue #9 (OPEN): Versioning web services. Dit heeft geen impact op standaard. Gaat starten, input vanuit ketenpartijen, resultaten in Q3/Q4.

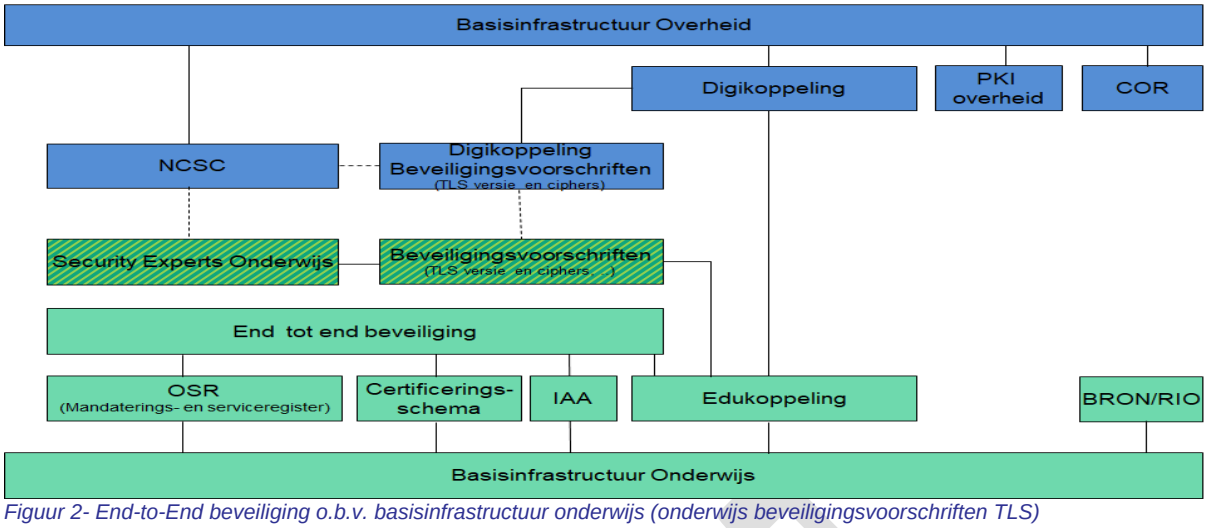
Issue #17 (OPEN): Vulling WSA:To in request niet obv wsdl-adres maar altijd met WSA anonymous vullen.
Dit lijkt niet wenselijk omdat platformen de WSA:To over het algemeen standaard vullen met het endpoint in de WSDL. Verder zou dit weer een extra afwijking zijn op de WSA tabel van Digikoppeling. Nu Digikoppeling ook het OIN optioneel toestaat in de WSA:To en WSA:From kan Edukoppeling deze tabel in geheel overnemen of hier naar verwijzen. Er wordt besloten dit issue af te voeren.

Issue #21 (OPEN): Certificaat controle door client.
Dit heeft geen impact op standaard, wordt onderdeel van best practices. Er wordt wel onderzocht of aansluiting met Digikoppeling en Edustandaard IBP werkgroep mogelijk is. We willen eenduidige beveiligingsmaatregelen om zeker te stellen dat een bepaald beveiligingsniveau gehaald wordt. De 2W-be TLS voorschriften zouden niet alleen voor Edukoppeling moeten gelden. Gaat starten, input vanuit ketenpartijen / IBP WG, resultaten in najaar.

Issue #22 (OPEN): TLS ciphers
Ciphers moeten ook voor andere ketens dan Edukoppeling hetzelfde zijn. Dit om problemen als voorheen met OSO te voorkomen. Het voorstel is om onderwijs beveiligingsvoorschriften voor basisprofielen op te stellen. Deze basisprofielen kunnen worden toegepast in OSO of Edukoppeling keten, maar mogelijk ook bij uitwisseling van persoonsgegevens in het IAA domein of REST georiënteerde standaarden.

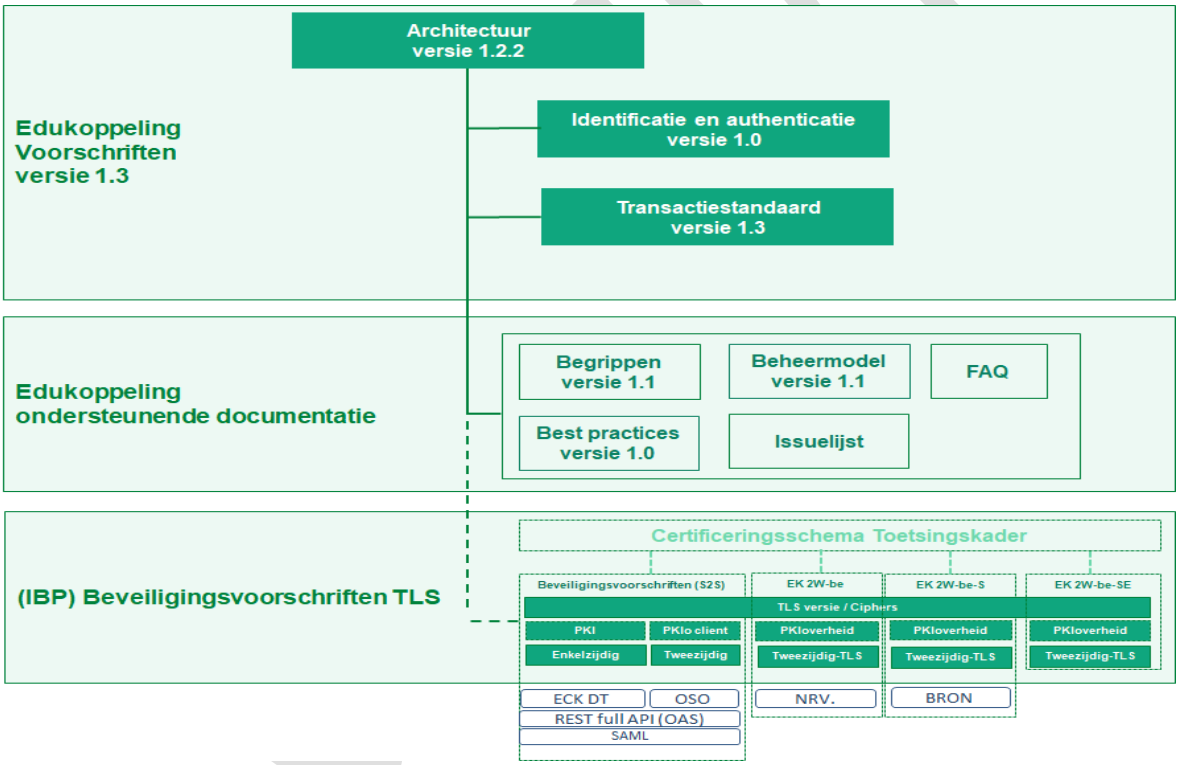
Issue 23 (OPEN): Uitwisselingspatronen met 1 of meer intermediairs beschrijven. Beschrijven in nieuwe versie best practices, mogelijk deels verwijzen naar Digikoppeling. Onderdeel Best practices versie 1.0.

Issue #28 (OPEN): In architectuurdocument schematisch bouwstenen onderwijs voor end-to-end beveiliging weergeven (figuur 11). Dit hangt mogelijk af van issue 22. We willen in het figuur kunnen aangeven waar beveiligingsvoorschriften TLS belegd zijn. Dit zijn nu nog de beveiligingsvoorschriften van Digikoppeling, maar dit blijft mogelijk problemen geven indien ketens een andere versie TLS of set ciphers voorschrijven. Het onderstaande figuur geeft e.e.a. schematisch weer. Hoe e.e.a. in figuur 11 van het Architectuurdocument wordt weergegeven zal de komende periode dus nog besloten moeten worden.



Figuur 2- End-to-End beveiliging o.b.v. basisinfrastructuur onderwijs (onderwijs beveiligingsvoorschriften TLS)

Het mogelijke resultaat voor de Edukoppeling documentatie wordt weergegeven in Figuur 3. Of dit voorstel overgenomen wordt en welke partij de beveiligingsvoorschriften TLS moet gaan beheren is nu nog onduidelijk.



Figuur 3 - Edukoppeling documentatie en beveiligingsvoorschriften TLS

3.3. Voorstel overige wijzigingen in documentatie

Een aantal voorstellen voor de nieuwe versie van de documenten wordt toegelicht.

- I&A document is onderdeel van standaard, voorschrift formaat OIN. De huidige conceptversie geeft niet aan dat de vulling van het OIN conform voorschrift moet. We willen in het definitieve document duidelijk stellen dat het formaat van het OIN een voorschrift is om te voorkomen dat dit identificerend kenmerk in verschillende ketens verschillend gebruikt gaat worden. De komst van RIO gaat impact hebben op dit voorschrift. Voordat RIO identiteiten in ketens gebruikt gaan worden, moet aangegeven zijn hoe hier binnen Edukoppeling mee omgegaan wordt.

- I&A document template idem aan architectuur en transactiestandaard. De huidige conceptversie is nog niet in lijn met de overige Edukoppeling documenten. Alle documenten die onderdeel van de standaard zijn hebben dezelfde inleiding etc.

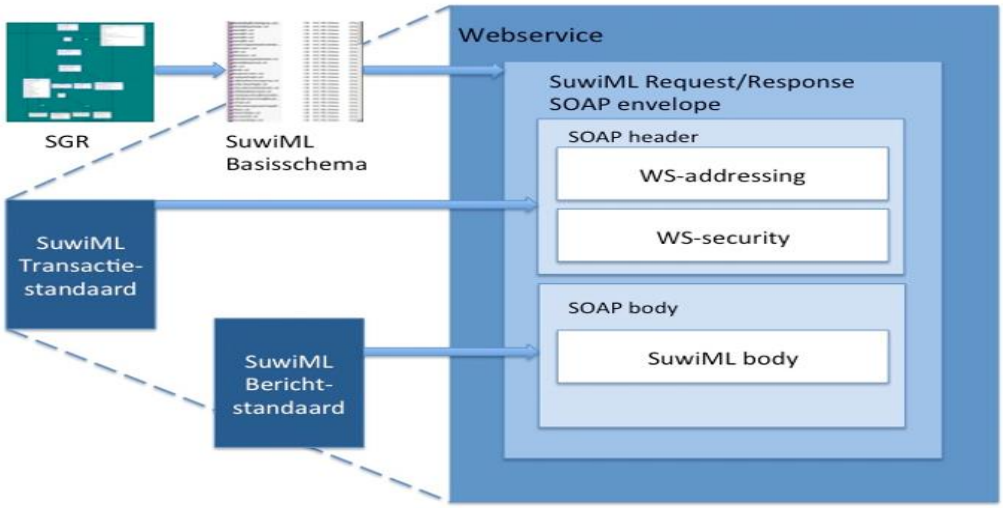
- Transactiestandaard en Architectuur verwijzen naar I&A, geen eigen OIN tabel. Waar relevant wordt vanuit de Transactiestandaard en Architectuur naar het I&A document verwezen.

- Architectuur bevat nu best practices. Ondertussen is er een apart best practices document. De best practices in architectuur worden verwijderd en in het best practices document opgenomen.

De werkgroep gaat akkoord met deze aanpassingen.

4. Toelichting Transactiestandaard Suwi keten

Binnen de wet Structuur uitvoering werk en inkomen (Suwi) zijn verschillende ketenpartijen belast met het uitvoeren van een wettelijke taak. Hierbij worden jaarlijks miljoenen berichten met privacygevoelige gegevens uitgewisseld. De nieuwe SuwiML Transactiestandaard beschrijft hoe de gestructureerde elektronische informatie-uitwisseling in deze keten ingericht gaat worden. Deze wordt beheerd door Bureau Keteninformatisering Werk & Inkomen (BKWI). De Transactiestandaard sluit aan op Digikoppeling en een SuwiML koppelvlakspecificatie moet zonder problemen goedgekeurd worden door de Compliancevoorziening van Logius.



Afbeelding 1 Opbouw berichten vanuit de Suwi standaarden

De Transactiestandaard bevat de volgende richtlijnen:

1. Afspraken worden expliciet vastgelegd in genummerde afspraken
2. De SuwiML Transactiestandaard conformeert zich aan de Requirements in het WS-I Basic Profile 1.1
3. Ieder SuwiML bericht heeft een SOAP Header met stuurinformatie.
4. **Om end-to-end secure gegevens uit te wisselen is signing verplicht bij een situatie als er tussen aanvrager en endpoint één of meer tussenstation(s) bevinden**.
5. De verbinding tussen twee partijen moet versleuteld worden d.m.v 2-zijdige TLS conform de richtlijnen van NCSC.
6. De koppelvlak specificaties van een web service worden vastgelegd in en bepaald door een WSDL beschrijving
7. Iedere Operation van een SuwiML webservice heeft zowel een Input als een Output
8. Iedere SuwiML webservice heeft een 'Document – Literal Wrapped' interface
9. Voor SuwiML webservices is de HTTP parameter SOAPAction leeg: “”
10. **SuwiML web services maken gebruik van WS-Addressing**

11. **Ten behoeve van het ondertekenen van onderdelen in berichten wordt in de WSDL gebruik gemaakt van WS-Policy.**
12. Eventueel gebruik van SuwiML stuurinformatie voor een web service wordt in de WSDL koppelvlak specificaties van die web service vastgelegd
13. Vertrouwelijke informatie wordt alleen verstrekt aan geautoriseerde partijen voor specifieke doelen.
14. Er gelden geen beperkingen aan de te gebruiken karakters anders dan dat ze tot de Unicode karakterset moeten behoren.
15. Bij het versturen van een Bericht dient de UTF-8 encodering gebruikt te worden
16. Alle partijen loggen zoeksleutels, de inhoud van de stuurinformatie, het tijdstip, en het adres waar een Bericht naar toe gaat of vandaan komt.
17. Stuurinformatie, sleutelwaardes en andere niet-vertrouwelijke informatie wordt tenminste bewaard volgens de gangbare wet en regelgeving.

Een aantal zaken die opvallen zijn het verplichten van het 2W-be-S profiel, het toepassen van WS-Policy en WS-Addressing Metadata[2] en een iets andere invulling van de WS-Addressing From header .

WS-Addressing Metadata

Met de WS-Addressing Metadata standaard kan in de WSDL aangegeven worden dat WS-Addressing headers verplicht zijn. Binnen het onderwijsdomein hebben we hiermee wel problemen ervaren op het Microsoft WCF platform.

WS-Policy

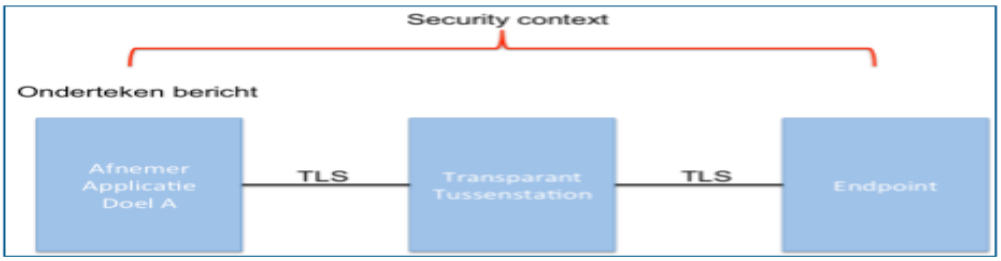
De WS-Policy biedt mogelijkheden om in de WSDL expliciet de beveiligingsmaatregelen voor het koppelvlak te definiëren, zoals het gebruik van tweezijdige TLS en het ondertekenen of versleutelen van berichtelementen. Ook het toepassen van WS-Addressing kan hiermee afgedwongen worden. Het is gewenst om in Edukoppeling verband de toepassing/interoperabiliteit hiervan nader te onderzoeken (de Suwi keten gebruikt over het algemeen andere platformen dan die binnen het onderwijs toegepast worden).

WSA:From

De WSA Headers worden vrijwel conform Digikoppeling gevuld. Wel is het OIN in de WSA:From en de WSA:To.verplicht. In het requestbericht wordt het WSA:From OIN gebruikt voor autorisatie. Het OIN in de respons wordt gebruikt t.b.v. logging. Naast het OIN wordt ook gebruik gemaakt van sub-OINs. Hiermee kunnen overheidsorganisaties fijnmaziger geïdentificeerd en geautoriseerd worden, bijvoorbeeld op het niveau van een afdeling, applicatie of wettelijke grondslag. Dit houdt in dat pér subOIN een aparte PKI-Overheid certificaat wordt toegepast.

Binnen de keten worden zowel transparante als niet-transparante intermediairs onderkend. Een uitwisseling met een transparante intermediair wordt gekenmerkt door de volgende eigenschappen:

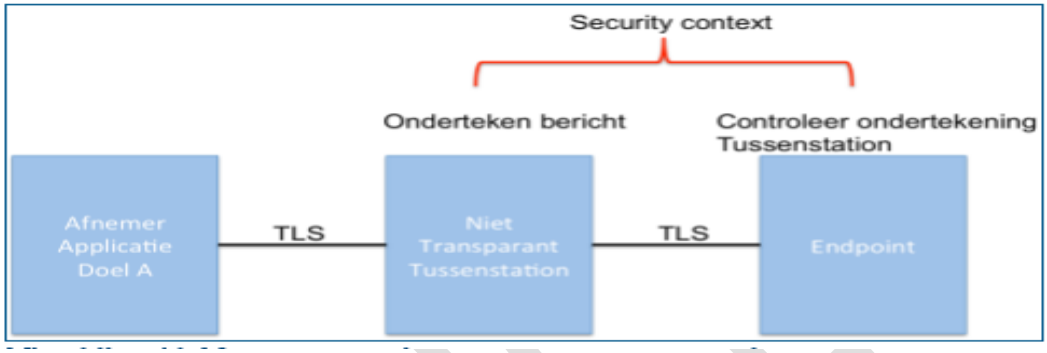
1. De applicatie/webservice ondertekend het bericht.
2. Elke afzonderlijke afnemer heeft zijn eigen identiteit in de vorm van een sub-OIN.
3. Van de afnemer tot aan het endpoint worden berichten uitgewisseld op basis van SuwiML
4. Het transparant tussenstation routeert het bericht naar het endpoint of eventueel naar een volgend transparant tussenstation. Het bericht kan en mag niet aangepast worden onderweg.



[2] http://www.w3.org/TR/ws-addr-metadata/

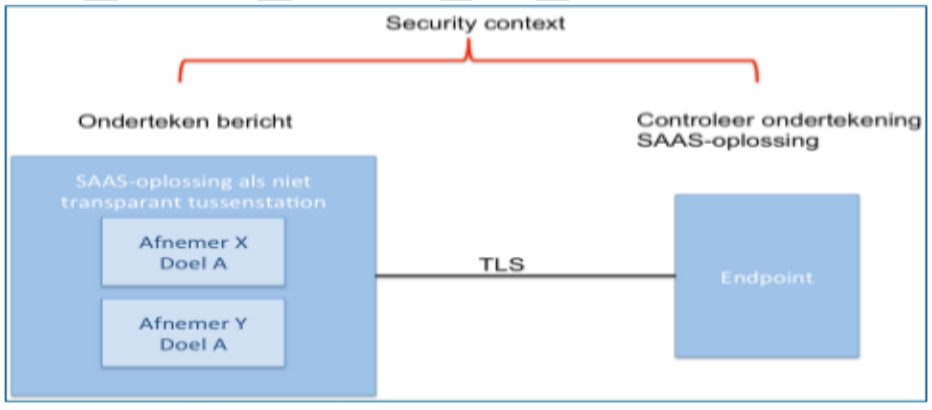
De gegevensuitwisseling met een niet-transparante intermediair wordt gekenmerkt door de volgende eigenschappen:

1. **Het niet transparante tussenstation ondertekent het bericht namens de applicatie**.
    a. Als het tussenstation zich binnen de afnemer in één omgeving bevindt dan zijn er geen aanvullende voorwaarden van toepassing.
    b. Als het tussenstation als een SAAS-oplossing afgenomen, moeten daar mogelijk aparte aanvullende afspraken gemaakt worden m.b.t. de beveiliging en de ondertekening van berichten.
2. Elke afzonderlijke afnemer heeft zijn eigen identiteit in de vorm van een sub-OIN.
3. Vanaf het tussenstation naar het endpoint wordt het bericht uitgewisseld op basis van SuwiML.
4. Vanaf de applicatie naar web service kan een intern protocol gebruikt worden, maar uiteraard ook SuwiML. Het tussenstation kan een SuwiML-adapter genoemd worden. Naast de SuwiML omzetting kan het tussenstation nog andere functionaliteiten bevatten.
5. Een niet transparant tussenstation kan ook via één of meer transparante tussenstations het endpoint bevragen



De gegevensuitwisseling met een niet-transparante intermediair in de vorm van een SaaS leverancier wijkt af van Edukoppeling en wordt gekenmerkt door de volgende eigenschappen:

1. **Het niet transparante tussenstation ondertekent het bericht namens de afnemer**[3].
2. Elke afzonderlijke afnemer heeft zijn eigen identiteit in de vorm van een sub-OIN.
3. Een SAAS-oplossing kan ook via één of meer transparante tussenstations het endpoint bevragen.



5. Rondvraag en sluiting

Geen punten meer voor de rondvraag. De volgende bijeenkomst is op woensdag 26 september van 10:00 tot 13:00.

[3] Het is op het moment van schrijven nog onduidelijk of hier bedoeld word dat het tussenstation dit doet met het eigen certificaat of dat van de afnemer. Dit bepaalt in hoeverre dit overeenkomt met de werking van Edukoppeling

Actielijst

#	Omschrijving	Status	Einddatum	Actie-houder	Prio
0024	Toelichting GB profiel	Nog inplannen	2018	BES/Erwin	3
0057	Onderzoeken problematiek met SOAP 1.1 en mogelijkheden om SOAP 1.2 binnen Edukoppeling/Digikoppeling toe te kunnen passen	Loopt, Digikoppeling onderzoek wordt afgewacht	Q3 2018	BES	2
0071	Wijzigingen nieuwe versie Edukoppeling op site publiceren (concept release notes).	Loopt, eerste inventarisatie o.b.v. issuelijst op 16 mei	Q3 2018	BES	2
0073	Onderzoek problematiek andere certs dan PKIo bij tls kanaal. Wat zijn consequenties	Afgehandeld	Q2 2018	BES	1
0074	Navraag bij Logius of er voor TLS, ondertekenen en versleuteling PKIo certs verplicht zijn	Afgehandeld	Q2 2018	BES	1
0075	Onderzoeken welke ketens grote bestanden (of gegevens in bulk) uitwisselen	Loopt (Geheugensteuntje: in Architectuurraad van 21-6 gaf CvTE aan dat zij hiermee bezig zijn).	2018	BES	3
0076	Onderzoeken PKI SAN en mogelijke alternatieven	Afgehandeld	Q3 2018	BES	2
77	Documenteren van push en pull variant	Nog inplannen	2018	BES	2
78	Overleg met Edustandaard over inrichten communityplatform	Nog inplannen	2018	Brian / Erwin	2
79	WG leden leden brengen release notes onder de aandacht in de verschillende ketens	Loopt	Q3/Q4 2018	WG leden	2

BES = Bureau Edustandaard
Grijs = afgehandeld of vervallen

Besluiten

#	Omschrijving	datum
1	Toepassingsgebied van de WUS wordt verbreed naar meldingen. WS-RM gaan we daarmee dus niet opnemen in de standaard als comply or explain-standaard (voor ebMS was dit al besloten). Mocht in het onderwijs WS-RM (of ebMS) toch nodig zijn voor bepaalde uitwisselingen, dan is het advies om dat eerst met de Edukoppeling WG te bespreken.	01-10-2014
2	Foutafhandeling: kijken wat het TO Digikoppeling gaat overnemen van project Utrecht en daarop foutafhandeling Edukoppeling baseren .	01-10-2014
3	Certificeringsschema: als onderwerp wel in de werkgroep Edukoppeling aan de orde laten komen om input te kunnen leveren, maar niet om het inhoudelijk het schema in zijn geheel te behandelen en te onderhouden. NB er wordt een aparte werkgroep binnen Edustandaard hiervoor opgericht die ook breder kijkt naar andere IB-aspecten.	01-10-2014
4	Voorleggen aan Architectuurraad of REST een kandidaat is om in Edustandaard te worden opgenomen. Daarbij ook laten bepalen waar (in welke werkgroep) dit het best belegd kan worden.	01-10-2014
5	Edukoppeling 1.2 wordt door de werkgroep geadviseerd om te gebruiken bij alle nieuw op te zetten uitwisselingen. Als het advies wordt overgenomen door de Standaardisatieraad op 2 juli dan is Edukoppeling 1.2 de voorgeschreven transactiestandaard. NB Standaardisatieraad heeft advies overgenomen vooruitlopend de formele acceptatie van de VDOD waarover op 2 juli nog geen uitsluitsel kon worden gegeven.	17-06-2015
6	In de werkgroep van 9-9-2015 heeft Ernst-Jan van Heusevelt namens de VDOD aangegeven dat de leden instemmen met Edukoppeling 1.2 als de te hanteren Transactiestandaard.	09-09-2015
7	Berichten moet kunnen worden geleverd op basis van een OIN gebaseerd op BRIN in de routeringsinformatie (WSA headers), een verdere verfijning in het OIN voor een automatische routering achter voordeur is niet gewenst,	14-12-2016
8	Van Beheermodel/Releasemanagement v0.3 kan een definitieve versie gemaakt worden en gepubliceerd met aanpassing die in de bijeenkomst van 8-2-2017 zijn aangegeven.	8-2-2017
9	Minor release 1.2.1 vastgesteld, stukken (Transactiestandaard, Architectuur, Begrippen) kunnen worden gepubliceerd.	21-6-2017
10	De laatste versie van de Best Practices document (0.2) kan worden gepubliceerd. Daarna van tijd tot tijd aanvullen/aanpassen op basis van input uit implementaties etc.	21-6-2017
11	Alle bestanden relevant voor een bepaald overleg worden op de site in een zip ontsloten	27-09-2017
12	Er kunnen onderwerpen geagendeerd worden die niet direct verband houden met de standaard zelf maar wel met de context van de standaard	27-09-2017
13	Er komt in 2019 een nieuwe medior versie van de standaard (1.3) waarin verduidelijkingen in documentatie worden opgenomen en zaken in lijn worden gebracht met wat nu al in implementaties de praktijk is op basis van eerdere afspraken/afstemming hierover. In 2018 worden de wijzigingen via release notes en conceptversie aangekondigd.	16-05-2018