

Concept Verslag ES werkgroep Edukoppeling transactiestandaard

Aanwezig: Peter Dam (Cito), Robert Kars (DUO), Gerald Groot Roessink (DUO), Marc Fleischeuers (Kennisset, BPV/Vroegtijdig aanmelden MBO), Brian Dommissie (Kennisset, voorzitter), Erwin Reinhoud (Kennisset/Bureau Edustandaard).

Afwezig: Edwin Verwoerd (Iddink, VDOD), Herrie Abbink (Educus)

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

Datum en locatie

16 mei 2018, 10:00-13.00 uur, Seats2Meet, Amersfoort

Agenda

1. Opening, mededelingen, vaststellen agenda
2. Doornemen verslag en actielijst
3. Terugkoppeling op hoofdlijnen uit Technisch Overleg Digikoppeling
4. Doornemen issuelijst (incl. bepalen wijzigingen voor versie 1.3)
Tevens bespreken van de volgende punten en bepalen of dit punten zijn om op te nemen op de issuelijst:
 - a. Bevindingen uit diverse implementaties en voorstel verbeteringen documentatie Edukoppeling (notitie van Marc Fleischeuers)
 - b. Nieuwe versie certificeringsschema
5. Voorstel voor onderzoek naar REST/JSON (concept projectvoorstel voor de Architectuurraad)
6. Implementatie-ondersteuning voor Edukoppeling en daarmee verwante zaken (memo vanuit SBB/saMBO-ICT)
7. Rondvraag / Sluiting

1. Opening, mededelingen, vaststellen agenda

Edwin Verwoerd en Herrie Abbink hebben zich afgemeld maar hebben input via de mail geleverd bij een aantal agendapunten.

Agenda wordt zonder wijzigingen vastgesteld.

2. Doornemen verslag en actielijst van 14 maart 2018

Er zijn geen opmerkingen op het verslag en deze wordt zonder wijzigingen vastgesteld.

Toelichting GB profiel (actiepunt #24)

Dit onderwerp heeft lage prioriteit. Zodra er hierom gevraagd wordt, of indien er een implementatie binnen het onderwijs is, zal dit onderwerp geagendeerd worden. Verder is het wenselijk om inzicht te hebben of er nu binnen het onderwijs grote berichten (> 20MB) uitgewisseld worden en hoe deze gegevensoverdracht is ingericht. Er

wordt een actiepunt toegevoegd om te onderzoeken waar en hoe nu grote berichten/bestanden uitgewisseld worden (#75).

Edukoppeling foutmeldingen (actiepunt #42)

In de huidige situatie zijn foutmeldingen een verplicht onderdeel binnen de transactiestandaard. De service provider moet de client over profiel-fouten informeren. Dit punt is later ook bij issue #16 besproken en er is besloten de foutmeldingen als onderdeel van de transactiestandaard te handhaven. De service providers moeten de client van informatie voorzien indien deze de fout heeft veroorzaakt, zodat deze de juiste maatregelen kan treffen om het probleem op te lossen. Service providers moeten de betreffende foutmeldingen dus implementeren en testen (zie ook issue #16). In Digikoppeling zijn deels dezelfde foutcodes opgenomen in de Digikoppeling Best Practices. We houden in de Edukoppeling transactiestandaard echter voorlopig een eigen lijst.

Onderzoeken problematiek met SOAP 1.1 (actiepunt #57)

Digikoppeling is ondertussen gestart met het onderzoek rond ondertekenen van berichten. Hierbij wordt met name ook naar het MS WCF platform gekeken. De resultaten worden najaar 2018 verwacht. Onderdeel van de deliverable is een referentie-implementatie. We willen hierna onderzoeken of deze ook geschikt kan worden gemaakt voor Edukoppeling. Hierna moet worden vastgesteld of dit voldoet of dat alsnog ook SOAP 1.2 toegepast moet kunnen worden.

Verwijderen van tijdelijk structuurdocument (actiepunt #67)

Nu er een *Digikoppeling overzicht actuele documentatie & compliance document*¹ is kan het Edukoppeling structuurdocument komen te vervallen, actiepunt #67 is afgehandeld. In de nieuwe release worden de verwijzingen in documentatie en site aangepast (issue #24).

Bij SBB navragen wat issues zijn met Edukoppeling (actiepunt #70)

De issues die bij SBB spelen worden bij agendapunt 4a besproken. Het actiepunt is hiermee afgehandeld.

Release notes nieuwe versie publiceren (actiepunt #71)

Op basis van de wijzigingen in de issuelijst wordt er een Edukoppeling versie 1.3 ontwikkeld. Dit wordt een versie met beperkte impact. Deze versie sluit beter aan op wat nu al bij implementaties toegepast wordt. Een voorbeeld hiervan is het vrijgeven van het te gebruiken poortnummer. In de nieuwe versie is poort 443 niet verplicht. De release notes beschrijven de wijzigingen die in deze nieuwe versie opgenomen worden.

Identificatie en authenticatiedocument, is suffix KvK verplicht '0000' (actiepunt #72)

Het OIN van private partijen (prefix is "00000003") moet de suffix "0000" bevatten. Private partijen kunnen dus (nu) niet een eigen suffix gebruiken om een bepaalde afdeling of dergelijks binnen de organisatie te identificeren. Het actiepunt is hiermee afgehandeld.

3. Terugkoppeling op hoofdlijnen uit Technisch Overleg Digikoppeling

Ciphers

Begin dit jaar is vanuit de onderwijssector aangegeven dat de Digikoppeling beveiligingsvoorschriften niet in lijn zijn met die van de onderwijssector. Dit had met name betrekking op de toegestane ciphers voor de TLS verbinding (issue #22). Naar aanleiding hiervan is bij het Technisch Overleg (TO) van 23 april de vraag gesteld hoe hier binnen Digikoppeling mee omgegaan moet worden. Logius presenteerde een voorstel om binnen Digikoppeling de toegestane ciphers op te nemen (een subset van NCSC). Het TO heeft echter besloten dat er eerst onderzocht moet worden of en binnen welke termijn de lijst met ciphers door NCSC geactualiseerd gaat worden en hoe het beheer van deze lijst is ingericht. De huidige is in 2014 opgesteld en sindsdien niet gewijzigd. Tijdens het TO Digikoppeling van 14 juni werd gemeld dat NCSC eind dit jaar met een nieuw overzicht komt met mogelijke ciphers. Daarnaast loopt bij TO Digikoppeling de discussie of er niet een aparte lijst voor S2S koppelingen moet worden opgesteld (de lijst van NCSC heeft een breder toepassingsgebied). We volgen de

¹ https://www.logius.nl/fileadmin/logius/ns/diensten/digikoppeling/digikoppeling_2.0/Digikoppeling_Overzicht_Actuele_Documentatie_en_Compliance_v1.0.pdf

ontwikkelingen bij Digikoppeling. Als de uitkomst hiervan niet past met wat de onderwijssector vereist zal de noodzaak hoger zijn om binnen het onderwijs een eigen lijst met ciphers te gaan beheren. Deze zou dan niet alleen voor Edukoppeling moeten gelden, maar ook voor ketens die nu nog geen Edukoppeling gebruiken maar wel TLS toepassen. Beheer moet dan belegd worden bij de werkgroep IBP van Edustandaard.

TLS 1.3

Ondertussen is er ook een nieuwe versie van TLS, versie 1.3². Er zullen hiermee tevens nieuwe ciphers toegepast gaan worden. Het is dus van belang dat bij het beheer van de lijst met mogelijke ciphers er niet alleen tijdig ciphers verwijderd worden, maar ook nieuwe tijdig opgenomen worden. Daarnaast moeten informatie hierover tijdig gepubliceerd worden zodat partijen tijdig actie kunnen ondernemen. Deze zullen echter wel afhankelijk zijn van de verschillende platformen en welke ciphers hierin ondersteund worden. Ook dit aspect zou in het in- en uitfasen van ciphers meegenomen moeten worden.

Versienummers Digikoppeling-documenten

Digikoppeling-documenten hebben een eigen versie en er wordt niet meer gewerkt met een overkoepelende versie. In plaats daarvan is er een document dat de samenhang van verschillende documenten weergeeft. Zo kan men bijvoorbeeld zien welke Digikoppeling documenten relevant zijn voor een WUS profiel. Deze wijze van versioning is ondertussen ook bij de pas-toe-of-leg-uit van Forum Standaardisatie³ doorgevoerd.

Signing

Bij het vorig overleg is aangegeven dat Logius in de Digikoppeling roadmap een onderzoek naar signing heeft opgenomen. Dit onderzoek is reeds gestart en heeft als doel om interoperabiliteitsproblemen bij het ondertekenen van berichten op te lossen.

REST

Er is al eerder gesproken over de ontwikkeling van REST koppelingen en hoe deze zich verhouden tot Edukoppeling. Naast dat hier recent ook bij de Edustandaard Architectuurraad over is gesproken (zie agendapunt #5), heeft dit ook de aandacht bij het TO Digikoppeling. Er werden een aantal ontwikkelingen rond REST toegelicht, zoals OAS⁴. Het is nog niet duidelijk wat precies de positie van Digikoppeling is. Er is eerst een inventarisatie nodig van wat men verwacht van Logius op dit gebied.

GB

We hebben het in de werkgroep nog niet eerder over het grote berichten profiel gehad. Dit mede omdat de noodzaak hiervoor tot op heden ontbreekt. Ook bij de overheid lijkt dit profiel weinig toegepast te worden. Recent heeft het Nationaal Archief echter dit profiel gebruikt om grote bestanden uit te wisselen. Hierbij is wel een push variant gebruikt in plaats van het standaard pull mechanisme. Hierbij is verder gebruik gemaakt van het ebMS profiel. Het plan is om de betreffende open source software beschikbaar te stellen.

OIN in WS-Addressing TO en FROM header

De Edukoppeling werkgroep heeft samen met een aantal TO Digikoppeling leden een wijzigingsvoorstel bij Logius ingediend. Die wijziging maakt het mogelijk om eventueel een OIN in de WS-Addressing To en From header op te nemen. Deze vulling is bij Edukoppeling verplicht, maar we hebben op dit punt nu wel een betere aansluiting op de Digikoppeling standaard. Logius heeft het voorstel overgenomen, maar er loopt nog een publieke consultatie. Zodra er een nieuwe versie is van de Digikoppeling WUS specificatie kunnen we eventueel de Edukoppeling-documentatie hier beter op laten aansluiten.

4. Doornemen issuelijst (incl. bepalen wijzigingen voor versie 1.3)

4.1. Bevindingen uit diverse implementaties en voorstel verbeteringen documentatie

Op basis van ervaringen bij een aantal projecten (de mutatieservice van SBB, kwalificatietest voor toegang tot de Nummervoorziening, ontwerp van Vroegtijdig aanmelden) zijn er een aantal situaties voorgekomen waarbij de

² <https://www.ietf.org/mail-archive/web/ietf-announce/current/msg17592.html>

³ <https://www.forumstandaardisatie.nl/standaard/digikoppeling>

⁴ <https://www.forumstandaardisatie.nl/sites/bfs/files/FS%20180425.3C%20Forum-advies%20OAS%203.0.pdf>

documentatie van Edukoppeling ruimte laat voor interpretatie waarbij er, als partijen verschillende interpretaties kiezen, er geen veilige en succesvolle gegevensuitwisseling plaatsvindt. Bij de interpretaties is de veiligheid van de gegevensoverdracht niet persé in het geding. Het verzoek vanuit de organisaties die te maken kregen met de interpretatieverschillen is om na te gaan of de documentatie van Edukoppeling zodanig is aan te passen dat de controles die plaatsvinden bij het valideren van requests en responses uitputtend worden beschreven, voorzien van een classificatie (verplicht, optioneel) en gekoppeld worden aan een beoogd niveau van beveiliging van de verbinding. De lijst hieronder is via een memo van Marc Fleischeuers die betrokken is bij die implementaties ingebracht.

De schriftelijke reactie van Edwin Verwoerd vooraf op deze lijst was dat wat hem betreft (en zijn achterban bij Iddink) deze aanbevelingen integraal overgenomen kunnen worden. Mocht het team er anders overdenken dan graag een onderbouwing en hoe deze issues dan zouden moeten worden opgelost met de wetenschap dat er hierbij ook rekening moeten worden gehouden met cloud partijen zoals Microsoft.

Herrie Abbink geeft in zijn mail vooraf aan dat hij akkoord is met de aanbevelingen, m.n. daar waar het gaat om bepaalde punten duidelijker in de standaard te beschrijven.

Ongewijzigd gebruik van het adres uit de wsa:to header in het http bericht

Er is een endpoint reference in de wsa:To header, dat sprekend lijkt op het adresveld in de https: headers waar het SOAP bericht in wordt verpakt en getransporteerd. Er zijn implementaties die de endpoint reference in de SOAP header ook gebruiken in de https: header. Dit kan onhandig zijn want de wsa:To header bevat volgens TS 3.4 ook het OIN van de formele partij van het antwoordbericht, dit komt dan ook terecht in de https: header. Dit kan bij de ontvanger weer leiden tot onnodige foutmeldingen, als deze niet rekent op additionele parameters in het request en ze niet kan verwerken.

Aanbeveling om in de [Transactiestandaard] p9 een zin op te nemen ter verduidelijking, bijvoorbeeld dat de vulling van het http 'To' veld waarschijnlijk anders is dan van het wsa:To veld en zeer waarschijnlijk geen oin-parameter zou moeten bevatten.

Aanbeveling wordt overgenomen (issue #25)

Controle op het TLS certificaat (logistieke laag): hoeft geen PKI te zijn.

Er is geen consensus rond deze stelling. Een aantal deelnemers is van mening dat voor Digikoppeling en hiermee ook voor Edukoppeling (waar vooralsnog ook ODOC certificaten gebruikt kunnen worden) PKI certificaten vereist worden. Er wordt een actie (#73) opgenomen om bij Digikoppeling navraag te doen. Hierna zal dit punt opnieuw besproken worden. Mede omdat de stelling is dat de TLS truststores nu niet expliciet zijn ingericht voor het gebruik van PKI Certificaten. Als er geen specifieke Edukoppeling TLS verbindingen kunnen worden gebruikt betekent dit mogelijk dat we het best effort profiel niet kunnen gebruiken voor identificatie en authenticatie. Dit zou er toe kunnen leiden dat er minimaal ook signing toegepast moet worden met een PKI certificaat.

Identity check failed for outgoing message.

Treedt op als er een verschil is tussen de CN in het certificaat en de (hostnaam van de) naam van de service, die optreedt zodra een service op virtuele infrastructuur draait (samen met X andere services). Partijen passen verschillende manieren toe om services te combineren achter een certificaat, en de strategie om de naam van een service te valideren (waar we zolang er nog geen goede public key infrastructuur is, nog aan vast zitten) moet hier rekening mee houden. Voor Edukoppeling gaat het hierbij om validatie van certificaten op logistiek niveau, waarbij de check uitgevoerd kan worden door infrastructuur, in elk geval buiten de directe controle van de applicatie die het bericht verwerkt. Dergelijke infrastructuur wordt in de regel geleverd door vendors en we verwachten dat internetstandaarden gevolgd worden, maar geen eigen (zelfs nationale) standaarden.

We hebben RFC's [2818], [5280] en [6125] met iets verschillende aanwijzingen over hoe namen van servers te valideren. Ze beginnen in elk geval bij het valideren van de servicenaam in de lijst met subject alternative names (indien aanwezig), en pas als last resort met de CN uit het certificaat. Voor geautomatiseerde clients (M2M) stelt RFC2818 dat er een melding in de log moet worden aangemaakt bij een geconstateerde niet-match, en dat deze client de verbinding Zouden moeten (SHOULD) verbreken. Het opstellen van een lijst met alternatieve namen aan de client-kant, zoals hier wel aanbevolen wordt, is niet een erkende methode volgens de internetstandaarden (en dat is ook goed voorstelbaar, gezien het onderhoud aan deze lijst dat door elke client moet worden

uitgevoerd!). Aanbeveling is om de strategie voor de validatie van de server-naam expliciet te maken in de documentatie van Edukoppeling en in lijn te brengen met de relevante internetstandaarden, en hierbij SANs in certificaten te betrekken.

De aanbeveling wordt niet overgenomen. De aanbeveling om de strategie voor de validatie van de server-naam expliciet te maken in de documentatie van Edukoppeling wordt overgenomen. Hoe hiermee om te gaan en of hiervoor SAN Certificaten voor toegepast moeten worden, zal nog onderzocht worden. Er wordt hiervoor een actiepun (74) opgenomen.

Firewall afscherming op IP-niveau.

SBB constateert bij het versturen van push-berichten naar instellingen dat een aantal instellingen gebruik maakt van firewalls met white lists voor inkomende berichten op ip-niveau. Nadat het ip-nummer van de dienst van SBB vanwege onderhoud was gewijzigd, kon de dienst een groot aantal berichten niet meer afleveren. Het is evident dat de infrastructuur van instellingen kwetsbaar is, en dat eenvoudige (white list) checks veel doen om ongewenst verkeer buiten te houden. Tegelijk zou het mogelijk moeten zijn om een policy af te spreken waarbij het toelaten van verkeer van erkende partners makkelijker en minder onderhoudsgevoelig is. Aanbeveling is om bijvoorbeeld samen met WG IBP en/of TO Continuïteit en beveiliging een passende maatregel uit te werken.

De aanbeveling levert geen wijzigingsverzoek en actie op voor Edukoppeling.

Validaties op pushberichten.

De choreografie van request-reply en push-ack berichtverkeer is identiek, maar de semantiek is net omgedraaid: bij request-reply is het informatieve deel van het bericht onderdeel van de reply, terwijl dat bij pushberichten onderdeel is van de push. Voor de ontvanger van een reply (met de gevraagde informatie) is het daarom zinvol om het bericht te valideren op integriteit en herkomst. Voor de verzender van een pushbericht is het een stuk minder zinvol om een acknowledgement van een pushbericht te valideren, de verwerking van de informatie (onderdeel van de push) heeft immers al plaatsgevonden. Wat is de informatieve waarde van een validatie op een ack, en wat zegt het als hierin niet alle berichtvelden gesigneerd zijn? Aanbeveling om in de beschrijving van validaties in de documentatie van Edukoppeling rekening te houden met de semantiek van de transactie, en de informatieve waarde die een validatie oplevert.

De aanbeveling wordt niet overgenomen. Wel wordt onderkend dat het expliciet onderkennen en documenteren van de verschillen wenselijk is (actiepun (77)). Er wordt echter besloten om geen specifieke subprofielen te definiëren waar andere validaties voor gelden. Zo kan een acknowledgement weer belangrijke info bevatten zoals een referentie of dergelijks. Dit zou weer een aanvullend subprofiel opleveren waar weer andere eisen aan gesteld worden. In de huidige situatie willen we het aantal profielen beperkt houden.

Berichtheaders bij gebruik van transparante routers.

Bij het ontwerpen van het berichtverkeer in het kader van vroegtijdig aanmelden (waarbij gebruik wordt gemaakt van transparante en niet-transparante routers tussen afzender en bestemming) is gebleken dat het niet gemakkelijk is om berichtverkeer zodanig te adresseren dat zowel routers als afzender en ontvanger hun werk kunnen doen. In Digikoppeling worden voor dit doel de ws-headers replyTo en faultTo gebruikt. Bij het inrichten van de diensten missen we nu met name de faultTo header. Berichten met fouten in de berichtinhoud (gemeentenummer of PGN niet bekend) worden pas bij de eindbestemming worden ontdekt, en de transacties om de berichten te versturen zijn dan al afgesloten. Dergelijke berichten moeten ofwel via een compleet nieuw in te richten apart kanaal worden verstuurd, of (zoals in deze situatie gekozen) handmatig worden opgevangen en verwerkt in samenwerking met de verzender. Concreet betekent dit voor Kennisnet, voor deze ene dienst, een geraamde maandelijkse inzet van circa 50 uur per maand voor supportmedewerkers. Aanbeveling: overweeg het verbod op faultTo op te heffen en documenteer het gebruik ervan in situaties met routing via intermediairs

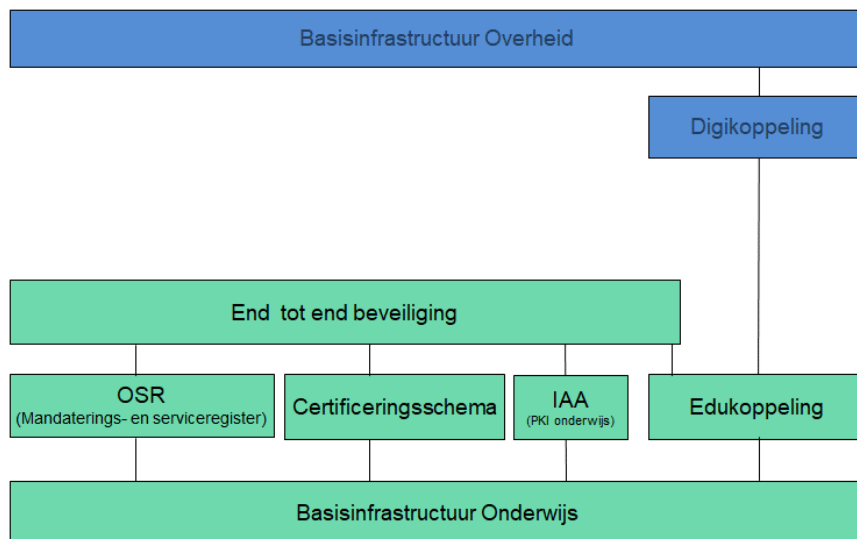
De aanbeveling wordt overgenomen. De WS replyTo en faultTo headers worden toegestaan. Vulling wordt overgenomen van de Digikoppeling tabel (issue #26). Hiermee wordt het gebruik van ReplyTo en FaultTo in het request toegestaan.

4.2. Nieuwe versie certificeringsschema

Al vanaf het begin wordt het certificeringsschema als onderdeel van de Edukoppeling-architectuur beschouwd. Beide verwijzen ook naar elkaar. Het certificeringsschema moet echter als zelfstandige bouwsteen gezien worden

dat mede met Edukoppeling end-to-end beveiliging mogelijk maakt. De nieuwe versie van het Certificeringsschema is ondertussen opgebouwd uit verschillende componenten met elk een eigen versie. Dit vraagt om een aanpassing van het architectuurdokument. Het wijzigingsvoorstel zal in de issuelijst opgenomen worden (#27)

Daarnaast wordt voorgesteld om in het architectuurdokument figuur 11 te vervangen door het onderstaande figuur. Hierin wordt weergegeven hoe op basis van verschillende bouwstenen end-to-end beveiliging gerealiseerd wordt. Het wijzigingsvoorstel zal in de issuelijst opgenomen worden (#28).



4.3. Issuelijst

#5 Onduidelijkheid welke elementen er ondertekend moeten worden bij 2W-Be-S en 2W-Be-SE profielen

Besluit: Issue wordt opnieuw behandeld. Zie agendapunt 3, het Digikoppeling onderzoek wordt afgewacht.

#8 Digikoppeling: Poort 443 is de standaard poort voor HTTPS verkeer.

Besluit: Voorstel is goedgekeurd en kan in de 1.3 versie meegenomen worden. Er wordt al met andere poorten dan 443 gewerkt in de nu werkende implementaties.

#9 Edukoppeling: Versioning

Besluit: Issue wordt opnieuw behandeld. Er wordt op basis van een inventarisatie bij ketenpartijen een best practice rond versioning opgesteld.

#10 Transactiestandaard WS-Addressing versie

Besluit: Voorstel is goedgekeurd. Deze wijziging wordt van Digikoppeling overgenomen en heeft geen impact. Er is een specificatie van 2006/05 (<http://www.w3.org/TR/2005/C%20R-ws-addr-core-20050817/>) en een verouderde specificatie van 2005/08 (<http://www.w3.org/TR/2005/CR-ws-addr-core-20050817/>). Digikoppeling schrijft het gebruik van de 2006/05 specificatie voor. Edukoppeling hoeft niet op dit punt aangepast worden, maar de wijziging bij Digikoppeling wordt wel bij release notes genoemd.

#15 Gebruik ODOC certificaten

Besluit: Voorstel is goedgekeurd. De ODOC certificaten worden nu eigenlijk alleen nog in IAA context gebruikt (in PO sector). Dit is een wezenlijk andere context dan waar de certificaten in de Transactiestandaard voor worden gebruikt. Het voorstel om de ODOC certificaten uit de Transactiestandaard te verwijderen wordt overgenomen. Deze kunnen overigens net als andere certificaten eventueel wel in testtrajecten toegepast worden.

#16 Aanpassing foutafhandeling

Besluit: Issue wordt afgevoerd. We handhaven de huidige situatie, zie ook bespreking actiepoint #42. Een aantal van de foutcodes die we in Edukoppeling voorschrijven zijn bij Digikoppeling in de Best Practices opgenomen. Bij Edukoppeling blijven de foutcodes verplicht en er blijft een eigen lijst in de Transactiestandaard staan. We houden deze wel zoveel mogelijk in lijn met elkaar.

#17 Vulling WSA:To in request

Besluit: Issue wordt opnieuw behandeld. Er moet nog onderzocht worden hoe we hier het beste mee om kunnen gaan. Digikoppeling gaat optioneel het OIN in WSA:To en WSA:From toestaan en hierna willen we tevens best practices opstellen rond routing (zoals het Edukoppeling SaaS-model). Hieruit volgt mogelijk een bepaalde keuze rond de vulling van WSA:To (naast dat hierin dus het OIN opgenomen wordt). Hierna zal in de werkgroep besproken worden hoe we hiermee binnen Edukoppeling willen omgaan.

#18 Foutcodes opnemen indien WS-A headers ReplyTo of FaultTo in bericht zijn opgenomen

Besluit: Issue wordt afgevoerd. Er is besloten dat WSA:ReplyTo en WSA:FaultTo gebruikt mogen worden (issue #26). Hiermee vervalt de noodzaak om deze foutmeldingen op te nemen.

#19 Transactiestandaard voorbeeld foutbericht (figuur 4) aanpassen.

Besluit: Voorstel is goedgekeurd. Dit wordt in de 1.3 versie meegenomen.

#20 Voorschriften rond vulling OIN

Besluit: Voorstel is goedgekeurd en reeds uitgevoerd bij de gegevensuitwisseling ihkv Doorontwikkelen BRON. In het Identificatie- en authenticatiedocument is nu de expliciete vulling opgenomen.

#21 Er is behoefte aan informatie rond gestandaardiseerde beveiligingsmaatregelen (CN verificatie).

Besluit: Issue blijft open. De noodzaak hiervoor is ook bij agendapunt 4.1 besproken. Omdat het gebruik van SAN's waarschijnlijk bij OSO niet is toegepast vanwege interoperabiliteitsproblemen is nader onderzoek nodig wat wenselijke alternatieven zijn.

#22 Beveiligingsvoorschriften ciphersuites

Besluit: Issue blijft open. Momenteel is dit issue in behandeling bij Digikoppeling en moet bij Edustandaard werkgroep IBP nog besproken worden.

#23 Uitwisselingspatronen met 1 of meer intermediairs beschrijven

Besluit: Issue blijft open. De best practices worden uitgewerkt. We willen hierbij in principe aansluiten bij Digikoppeling waar ook best practices rond routing ontwikkeld worden.

#24 Digikoppeling 3.0 is vervallen, verwijzen naar specifieke Digikoppeling documenten

Besluit: Voorstel is goedgekeurd. Alle verwijzingen naar DK 3.0 kunnen uit documentatie verwijderd worden. Het Digikoppeling document *Overzicht_Actuele_Documentatie_en_Compliance* geeft aan welke Digikoppeling documenten relevant zijn voor het WUS-profiel.

#25 Documenteren onderscheid tussen WSA:To en HTTP header

Besluit: Aanbeveling bij 4.1 wordt overgenomen. In de Transactiestandaard wordt opgenomen dat de vulling van het http 'To' veld waarschijnlijk anders is dan van het wsa:To veld en geen oin-parameter zou moeten bevatten.

#26 ReplyTo en FaultTo mogen in request opgenomen worden

Besluit: Het nieuwe voorstel om het gebruik van WSA:ReplyTo en WSA:FaultTo is goedgekeurd. We volgen hierin wat Digikoppeling voorschrijft.

#27 Aanpassing architectuur document: Verwijzing naar het certificeringsschema aanpassen

Besluit: Voorstel wordt overgenomen, zie ook 4.2.

#28 Aanpassing architectuurdokument: figuur 11 O.a.de verwijzing naar het certificeringsschema wordt aangepast. Voorstel zal opnieuw besproken worden.

5. Voorstel voor onderzoek naar REST/JSON

In de Architectuurraad wil graag een onderzoeksproject starten naar REST en heeft gevraagd om een projectvoorstel dat zij naar de Standaardisatieraad willen sturen met het verzoek dit project te starten. De werkgroep Edukoppeling wordt gevraagd om het concept te reviewen en aan te vullen en tevens na te denken hoe en door wie dit onderzoek het beste kan worden uitgevoerd. Vanuit de werkgroep wordt aangegeven dat dit onderzoek wenselijk is. Er lopen verder verschillende trajecten binnen de onderwijssector en bij de overheid die hier raakvlakken mee hebben. Deze worden tevens in het voorstel benoemd. Waar dit project belegd moet worden is nu nog niet duidelijk. De werkgroep gaat er wel vanuit dat deze geconsulteerd wordt en betrokken is bij de review van de resultaten.

Reactie van Herrie Abbink vooraf via de mail is met het bovenstaande in lijn: "Ik onderschrijf het breder gebruik van REST API's; bij EduArte niet alleen mobiele apps maar ook portalen voor student, docent, ouder en bedrijf. Nader onderzoek is dan ook zeer wenselijk."

6. Implementatie-ondersteuning voor Edukoppeling

Implementatie-ondersteuning is door de Edustandaard werkgroep Edukoppeling al eerder onderkend als nuttig en wellicht noodzakelijk. Veel vragen en issues worden nu al door de standaardisatiewerkgroep opgepakt, maar er zitten grenzen aan wat binnen de huidige resources mogelijk is, zowel qua beschikbare tijd als benodigde kennis. De werkgroep besluit dan ook deze ontwikkeling te ondersteunen. Over de precieze taakstelling en vereisten van het uitvoerende gremium, de afbakening met wat er nu al gedaan is in de Edustandaard-werkgroep en hoe de relatie tussen beide standaardisatiewerkgroep en ondersteunend gremium er uit moet gaan zien is echter nog niet duidelijk. De opstellers wordt gevraagd om het memo op deze punten aan te scherpen.

Reactie van Herrie Abbink vooraf via de mail: "Ik herken de problematiek en sluit mij aan bij de vraagstelling; ook als leverancier is het vaak een zoektocht waar concreet ondersteuning gevonden kan worden. Wat betreft de invulling kan ik vanuit onze ervaring mogelijk een bijdrage laten leveren op het gebied van kennisdeling (is nog geen concrete toezegging)."

7. Rondvraag

Geen.

8. Sluiting

De volgende bijeenkomst is op 4 juli van 10:00 tot 13:00.

Actielijst

#	Omschrijving	Status	Einddatum	Actie-houder	Prio
0024	Toelichting GB profiel	Nog inplannen	2018	BES/Erwin	3
0042	Edukoppeling foutmeldingen agenderen en in WG bespreken	Afspraak is dat huidige situatie wordt gehandhaafd, punt kan derhalve nu afgevoerd worden	Q3 2018	BES	2
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
0067	Verwijderen van tijdelijk structuurdocument, documenten controleren op eventuele verwijzingen naar Digikoppeling 3.0. en verwijzing naar het Digikoppeling overzicht actuele documentatie & compliance opnemen	Afgehandeld, wordt in nieuwe release verwerkt (issue #24)	Q1 2018	BES	1
0070	Bij SBB navragen wat issues zijn met Edukoppeling	Afgehandeld, agendapunt 4a	Q2 2018	BES	1
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
0072	Identificatie en authenticatiedocument, suffix kvk nummer vrij in te vullen of verplicht "0000".	Afgehandeld, OIN met KvK nummer heeft altijd "000" als suffix.	Q2 2018	BES / Gerald	1
73	Onderzoek problematiek andere certs dan PKI bij tls kanaal. Wat zijn consequenties				
74	Navraag bij Logius of er voor TLS, ondertekenen en versleuteling PKI certs verplicht zijn		Q2 2018	BES	1
75	Onderzoeken welke ketens grote bestanden (of gegevens in bulk) uitwisselen	Nog inplannen (Geheugensteuntje: in Architectuurraad van 21-6 gaf CvTE aan dat zij hiermee bezig zijn).	2018	BES	3
76	Onderzoeken PKI SAN en mogelijke alternatieven	Nog inplannen	Q3 2018	BES	2
77	Documenteren van push en pull variant	Nog inplannen	2018	BES	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 uitsluitel 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 routing 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