

De document bevat de reeds bekende issues behorend bij de Afspraak Edukoppeling. De issues worden beschreven in een onderstaande tabel. De laatste drie kolommen (Prioriteit, Complexiteit en Impact) zijn indicaties vanuit Edustandaard. De kolommen van deze tabel hebben de volgende betekenis:

1. "Nr": Administratief gegeven om naar het issue te kunnen refereren. Dit is een volgnummer in de lijst om bij bespreking van deze lijst eenduidig naar het issue te kunnen verwijzen.
2. "Ingediend": De gegevens in deze kolom omvatten de datum van indiening en de indiener. Deze gegevens kunnen worden gebruikt om de achtergrond of nadere details van het issue later te kunnen achterhalen.
3. "Issue": De omschrijving van het issue in de derde kolom bevat een beknopt, relevant omschrijving van het issue. Indien het issues via de e-mail wordt ingediend, wordt de relevante tekst uit de e-mail overgenomen. De eerste onderstreepte regel bevat een kort, inhoudelijk samenvattend label van het issue.
4. "Status": Bij ieder issue wordt de status in deze kolom bijgehouden. De mogelijke waarden in deze kolom en bijbehorende betekenis zijn:

Waarde van Status	Betekenis
Niet uitgewerkt	Dit issue is ingediend en geregistreerd, maar nog niet boeerdeld door Edustandaard.
Beoordeeld	Issue is door Edustandaard ingeschat als relevant voor bespreking met werkgroep; dit issue wordt naar prioriteit ingepland voor werkgroep.
Toestemming voor verdere uitwerking	Het issue is in werkgroep besproken en er is toestemming gegeven om impact op standaard uit te werken in de vorm van een RFC.
Uitgewerkt tot RFC	Het RFC is uitgewerkt en is gereed voor beoordeling door werkgroep
Opnieuw behandelen	De werkgroep heeft aangegeven dat er geen besluit kan worden genomen. De RFC moet op punten aangepast worden en opnieuw worden behandeld.
Voorwaardelijke goedkeuring	Het RFC is door werkgroep onder voorbehoud goedgekeurd, bijvoorbeeld indien dit samnhangt met een ander nog te beoordelen issue. Op basis van een voorwaardelijke goedkeuring kan een item niet in release opgenomen worden.
Goedgekeurd	Het RFC is door werkgroep goedgekeurd. De wijziging wordt in de aangegeven release opgenomen.
Afgewezen	Het Idee of RFC zal niet (langer) door het Edustandaard of Werkgroep in behandeling genomen worden, het wordt niet in releasplan opgenomen.

5. "Prio": Bij ieder issue wordt een inschatting gemaakt van de prioriteit bij betrokkenen om het issue opgelost te krijgen. Deze inschatting is relatief, dus t.o.v. andere issues. De mogelijke waarden in deze kolom zijn: Laag, Gemiddeld of Hoog. Hierbij kan tevens de afgesproken release aangegeven worden.
6. "Complex": Bij ieder issue wordt een inschatting gemaakt van de complexiteit van het proces om te komen tot één oplossing die eenduidig is en draagvalk heeft. Deze inschatting is relatief, dus t.o.v. andere issues. De mogelijke waarden in deze kolom zijn: Laag, Gemiddeld of Hoog.
7. "Impact": Bij ieder issue wordt een inschatting gemaakt van de impact voor partijen om de oplossing te implementeren. Deze inschatting is indicatief en kan per partij anders zijn. De mogelijke waarden in deze kolom zijn: Laag, Gemiddeld of Hoog.
8. "Categorie": Bij ieder issue wordt de categorie in deze kolom bijgehouden. De mogelijke waarden in deze kolom en bijbehorende betekenis zijn:

Waarde van Categorie	Betekenis
1	Tekstuele correcties en verduidelijkingen
2	Functionele correcties en verduidelijkingen
3	Kleine functionele aanpassingen
4	Substantiële functionele aanpassingen

Nr	Ingediend	Beschrijving	Status	Prioriteit	Complex	Impact	Categorie
23	Kennisnet	<p>Uitwisselingspatronen met 1 of meer intermediairs beschrijven</p> <p>In de architectuur worden verschillende uitwisselingspatronen beschreven. Er ontbreekt een beschrijving van uitwisselingspatronen met bijvoorbeeld 1 of meer intermediairs (knooppunten).</p> <p>In de vroegtijdig aanmelden-keten zijn er meerder intermediairs en is de vraag naar voren gekomen hoe asynchroon inhoudelijke fouten naar de initiële bron gecommuniceerd kunnen worden.</p> <p>Voorstel:</p> <p>Uitwisselingspatronen met intermediairs in architectuurdocument opnemen en beschrijven hoe Edukoppeling in deze context gebruikt wordt. Analyseren of Edukoppeling voldoende ondersteuning biedt, of er aanvullende informatie in de vorm van best practices nodig is of dat er een wijziging van de standaard nodig is.</p> <p>Ook bij Digikoppeling zijn hier ontwikkelingen. Het optioneel opnemen van het oin in wsa:To en wsa:From is bedoeld om routing via intermediairs expliciet te maken. Als het Digikoppeling/WUS-koppelvlak hierop is aangepast is het wenselijk dat in het Digikoppeling Best Practices WUS document bijvoorbeeld het SaaS-model wordt beschreven.</p> <p>Edukoppeling Werkgroep 10-10-2018: Onderdeel Best practices versie 1.0. Oplevering BP 1.0 gepland voor Q1 2019.</p> <p>Update: Omdat de ontwikkeling bij Digikoppeling op dit vlak niet zo snel verloopt, zijn de best practices van Edukoppeling wel al vernieuwd en als 1.0 gepubliceerd. Als Digikoppeling zover is met de beschrijving dan sluiten we met Edukoppeling Best Practices daarop aan. Vanuit Edukoppeling werkgroep zal met Digikoppeling samengewerkt worden op dit punt.</p> <p>Besluit:</p>	In behandeling	Midden	Midden	Midden	1
44	WG	<p>Upgrade naar SOAP 1.2</p> <p>Vanuit ketens komen signalen dat een SOAP 1.2 implementatie op het</p>	Open	Midden	Hoog	Hoog	4

		<p>.Net platform makkelijker is dan op basis van SOAP 1.1. Eerder is dit als actiepunt genoteerd, maar is nu opgenomen als issue.</p> <p>De overstap naar SOAP 1.2 is een logische doorontwikkeling van het WUS profiel, maar in principe onwenselijk als Digikoppeling niet ook deze stap maakt. Voorlopig lijkt dit geen prioriteit te hebben bij Digikoppeling. Het kan wel helpen als er vanuit Edustandaard onderzoek gedaan wordt naar de impact op de Edukoppeling (Digikoppeling) standaard. De verwachting is namelijk dat deze vrij groot is, het heeft impact op het hele stelsel van afspraken (WSDL/ WSA en WSS) en de keuzes die op basis van een WS-I Basic Profile zijn gemaakt (voor SOAP 1.2 worden andere basic profiles gebruikt). Als de impact in theorie is bepaald is het van belang om ook de implementeerbaarheid op verschillende platformen te toetsen, zodat ook vastgesteld kan worden dat SOAP 1.2 inderdaad voordeel oplevert. Dit alles zal dus redelijk wat effort vragen.</p> <p>Voorstel</p> <p>Omdat we nu voor .Net ook code beschikbaar stellen is de verwachting dat partijen hiermee een SOAP 1.1 implementatie makkelijker kunnen realiseren. Er is ondertussen ook een community platform dat partijen die problemen ervaren kunnen gebruiken. Het idee is om ook .Net experts lid te maken van dit platform.</p> <p>Besluit</p> <p>WG 13 maart 2019: voorlopig nog geen actie. Dit krijgt hogere prioriteit bij meerdere signalen vanuit keten.</p>					
45	WG	<p>Edukoppeling Compliancevoorziening</p> <p>Er is behoefte aan een Edukoppeling compliancevoorziening (zie actiepunt #84). Mogelijk kan tot die er is de compliancevoorziening van Digikoppeling gebruikt worden.</p> <p>Voorstel</p> <p>Een compliancevoorziening voor Edukoppeling beschikbaar stellen. Dit heeft geen impact op de standaard zelf en dient enkel ter ondersteuning van implementaties.</p> <p>Besluit</p>	Open	Midden	Laag	Laag	1

48	BES	<p>Aanpassing Digikoppeling gebruiksvoorwaarden (release notes 20210111): Private partijen kunnen ten behoeve van (SAAS-) dienstverlening aan hun publieke klanten SubOIN's aanvragen</p> <p>Zie https://www.logius.nl/sites/default/files/bestanden/website/20210111_Release_Notes_Wijziging_Digikoppeling_Standaard_documentatie.pdf</p> <p>We moeten de impact bepalen. Het is belangrijk een expliciet besluit te nemen of we andere identiteiten kunnen/willen gebruiken in SaaS-profiel</p> <p>Besluit</p>	Open	Midden	Midden	Midden	4					
49	BES	<p>SaaS Profiel foutmelding 'Niet gemandateerd'.</p> <p>In het REST/SaaS-profiel is een fout opgenomen om aan te geven dat een partij niet gemandateerd is. Het voorstel is om voor het WUS-profiel ook een foutmelding op te nemen (SOAP FAULT statuscode 501).</p> <p>Voorstel</p> <table border="1"> <tr> <td>23</td> <td>TLS: OIN in certificaat niet gemandateerd om voor school (From routeringskenmerk) in context van deze service gegevens uit te wisselen</td> <td>Syntax fout of nieuwe Categorie 'Mandatering'</td> <td>EK</td> <td>De partij die deze gegevens wil uitwisselen in de context van deze service is niet door de betreffende Eindorganisatie (WSA:From) gemandateerd</td> </tr> </table> <p>Besluit</p>	23	TLS: OIN in certificaat niet gemandateerd om voor school (From routeringskenmerk) in context van deze service gegevens uit te wisselen	Syntax fout of nieuwe Categorie 'Mandatering'	EK	De partij die deze gegevens wil uitwisselen in de context van deze service is niet door de betreffende Eindorganisatie (WSA:From) gemandateerd	Open	Midden	Laag	Laag	3
23	TLS: OIN in certificaat niet gemandateerd om voor school (From routeringskenmerk) in context van deze service gegevens uit te wisselen	Syntax fout of nieuwe Categorie 'Mandatering'	EK	De partij die deze gegevens wil uitwisselen in de context van deze service is niet door de betreffende Eindorganisatie (WSA:From) gemandateerd								
50	Kennisnet	<p>Edukoppeling Begrippen: aansluiten op de ROSA</p>	Open	Midden	Laag	Laag	1					

		<p>Begrippenlijst van Edukoppeling stamt uit 2017 en zou moeten worden herzien, o.a. tav de begrippen "dienst" en "service", die qua scope en definitie niet aansluiten bij bijv. de NORA en bij diensten als OSR. Zelf een update doorvoeren is een optie, echter er draait in 2021-2022 een project bij Edustandaard getiteld Revisie ROSA waarin onder andere een centrale begrippenlijst onderdeel van gaat uitmaken. Aangezien veel begrippen niet specifiek horen bij Edukoppeling is een andere optie om geen eigen begrippenlijst meer bij te houden en te publiceren als onderdeel van de documentatie, maar te verwijzen naar de ROSA-begrippen en op terreinen waar in de werkgroep kennis van aanwezig is, mee te helpen die centrale begrippenlijst kwalitatief en kwantitatief up-to-date te houden.</p> <p>Besluit Werkgroep 14-9-2021: Begrippenlijst niet zelf meer bijhouden maar verwijzen naar ROSA-begrippenlijst (in wording). Daarom nu geen aanpassingen al doorvoeren in huidige Edukoppeling-begrippen.</p>					
51	WG	<p>Beschrijven van verschillende varianten hoe een mandateringsverificatie uitgevoerd kan worden</p> <p>Tijdens het overleg van 14 september 2021 is door de werkgroep besloten om niet expliciet op te nemen dat een mandateringsverificatie verplicht is. Dit omdat het voor een groot deel ook iets voor een ketenafpraak is.</p> <p>We willen validatie niet verplicht stellen in profielen maar wel de mogelijkheden beschrijven. Zoals de huidige mogelijkheden via het bevragen van OSR, of zoals DUO doet door periodiek batchgewijs OSR gegevens op te halen. Ook mogelijkheden onderzoeken hoe dit bijvoorbeeld als token meegestuurd kan worden in de berichtuitwisseling.</p>	Open	Laag	Midden	Midden	4
52	BES	<p>Toepassingsgebied aanpassen. Aansluiten op wijziging in toepassingsgebied van Digikoppeling. Dit heeft geen impact en is enkel een verduidelijking</p> <p>FS toepassingsgebied DK is het volgende geworden:" Digikoppeling moet worden toegepast bij digitale gegevensuitwisseling die plaatsvindt met voorzieningen die onderdeel zijn van de GDI, waaronder de basisregistraties, of die sector-overstijgend is. De verplichting geldt voor gegevensuitwisseling tussen systemen waarbij er noodzaak is voor tweezijdige authenticatie.</p> <p>Voorstel</p>	Goedgekeurd Meenemen in volgende Release	Laag	Laag	Laag	1

		<p>Bij Edukoppeling de volgende toevoeging opnemen: "waarbij er noodzaak is voor tweezijdige authenticatie."</p> <p>Besluit 14 september 2021: Meenemen in volgende versie van documenten waarin het toepassingsgebied genoemd wordt.</p>					
53	BES	<p>Verschillend gebruik niet normatieve API Design rules in Edukoppeling REST/SaaS-profiel en Digikoppeling REST</p> <p>Het Edukoppeling REST/SaaS-profiel is opgesteld voordat er een Digikoppeling REST-profiel beschikbaar was. Ondertussen is die er wel en beide maken gebruik van de Kennisplatform API Design rules, maar er zijn verschillen.</p> <p>De Kennisplatform API Design rules bestaat nu uit normatieve (vastgestelde) en informatieve (nog niet vastgestelde) Extensies. In het Edukoppeling REST/SaaS-profiel zijn ook informatieve extensies¹ opgenomen zodat we in het REST-profiel een compleet overzicht houden. Deze extensies zijn echter nog wel in ontwikkeling en sinds het opstellen van het REST/SaaS-profiel hebben er ook wijzigingen plaatsgevonden. Er zijn ondertussen principes verwijderd en er zijn ook principes bijgekomen. Het Digikoppeling REST-API profiel maakt alleen gebruik van het normatieve deel van de REST-API Design Rules². Er wordt een wijzigingsvoorstel voor het REST/SaaS-Profiel opgesteld om in de volgende werkgroepbijeenkomst (19-1-2022) te bespreken en over te besluiten.</p> <p>Voorstel Wijzigingsvoorstel REST-SaaS-profiel.pdf (moet nog worden gepubliceerd).</p> <p>Besluit</p>	Open	Midden	Midden	Midden	3

¹ Gepubliceerde versie [API Designrules Extensions \(Nederlandse API Strategie IIb\) \(geostandaarden.nl\)](https://geostandaarden.nl), Werkversie [API Designrules Extensions \(Nederlandse API Strategie IIb\) \(geonovum.github.io\)](https://geonovum.github.io)

² Het is verplicht te voldoen aan alle (normatieve) eisen van de REST-API Design Rules

ARCHIEF

Nr	Ingediend	Beschrijving	Status	Prioriteit	Complex	Impact	Categorie
1	Kennisnet	<p>Transactiestandaard: Paragraaf 3.4 Identificatie via WS-addressing header en Paragraaf 3.5 Foutafhandeling: WSA:ReplyTo</p> <p>Het voorkomen van de WSA:ReplyTo in request levert fouten op bij implementaties. In de tabel 3.4 Identificatie via WS-addressing header staat nu "WSA:ReplyTo: Wordt niet gebruikt". Partijen interpreteren dit dat het een keuze is of ReplyTo wel of niet opgenomen kan worden in request.</p> <p><u>Voorstel:</u></p> <p>a. Extra foutmelding in de lijst van paragraaf 3.5 (foutafhandeling) opnemen, #23 "WSA:ReplyTo mag niet voorkomen in het request" .</p> <p><u>Besluit (dec 2016):</u></p> <p>Issue blijft open, de foutmelding (item a) wordt pas bij een volgende medior of major release meegenomen.</p> <p><u>Besluit (juni 2017):</u></p> <p>Hetzelfde geldt voor FaultTo, dit issue wordt afgewezen en wordt samen met FaultTo in Issue #18 opgenomen.</p>	Afgewezen	Midden	Laag	Laag	2
2	DUO	<p>Transactiestandaard: 3.5 Foutafhandeling, typo</p> <p><u>Voorstel:</u></p> <p>In voorbeeld van foutmelding staat tekstuele fout, "SOAP:Envelop" moet zijn "SOAP:Envelope"</p> <p><u>Besluit:</u></p>	Goedgekeurd	Midden	Laag	Laag	1

		Verwerken in versie 1.2.1					
3	DUO	<p>Transactiestandaard: Paragraaf 3.4 Identificatie via WS-addressing header: Voorbeeld OIN in WSA-header</p> <p>Edukoppeling geeft aan dat messageID een UUID moet zijn. Volgens de WSA-specs moet een WSA:MessageID echter een URI/IRI zijn.</p> <p><u>Voorstel:</u></p> <p>Het voorbeeld aanpassen: UUID wordt vooraf gegaan door urn:uuid:</p> <pre><wsa:MessageID>urn:uuid:91576FE2-4533-43CB-BFA1-51D2B631453A</wsa:MessageID></pre> <p><u>Besluit:</u></p> <p>Verwerken in versie 1.2.1</p>	Goedgekeurd Release 1.2.1	Midden	Laag	Laag	1
4	DUO	<p>Transactiestandaard: 3.5 Foutafhandeling: Opbouw foutbericht</p> <p>Wat wordt onder het SOAP:Fault voorbeeld bedoeld met de zin: "Het foutbericht wordt dus verpakt in het retourbericht onder dezelfde naam als het goedbericht. Er wordt daarmee geen gebruik gemaakt van een speciale WSDL-faultoperatie". Raar want in de DK voorbeelden wordt in de WSDL wel degelijk een aparte SOAP:Fault operatiennaam opgenomen. Wat is het verschil?</p> <p><u>Voorstel:</u></p> <p>Rationale voor deze tekst ontbreekt. Tekst verwijderen</p> <p><u>Besluit:</u></p> <p>Verwerken in versie 1.2.1</p>	Goedgekeurd Release 1.2.1	Midden	Laag	Laag	1
5	DUO	<p>Digikoppeling: Onduidelijkheid welke elementen er ondertekend moeten worden bij 2W-Be-S en 2W-Be-SE profielen</p> <p>Er is onduidelijkheid welke gegevens gesigned moeten worden in het profiel Edukoppeling Be-S/Be-SE. Daarnaast is het onduidelijk of velden</p>	Afgewezen (issue is afgehandeld, geen wijziging)	Midden	Midden	Midden	1-2

	<p>afzonderlijk of in zijn geheel signed moeten worden. De documentatie moet hierop verbeterd worden om discussies te vermijden.</p> <p>Alle WSA: velden, timestamp en body moeten apart signed worden. Alleen door alle velden te signen kan non-repudiation en integriteit gegarandeerd worden. Door velden los te ondertekenen wordt het valideren minder foutgevoelig omdat o.a. volgorde van deze velden in de header er dan niet toe doet. Bovendien zou je anders de gehele header moeten signen maar in dat geval kun je in voorkomende gevallen in een keten nooit (technische) headerblocks toevoegen mocht dat nodig zijn.</p> <p><u>Voorstel:</u></p> <p>Onderzoeken of de omschrijving bij digikoppeling aangepast kan worden. Anders kan het misschien expliciet in Edukoppeling bij het 2W-Be-S en 2W-Be-SE profiel voorschrijven.</p> <p>WG dec 2016: Issue is besproken maar blijft open. Het zal eerst in Digikoppeling verband besproken worden. Nader besluit volgt na terugkoppeling vanuit Digikoppeling</p> <p>Wergroep 16 mei 2018: We wachten op reslutaten van het onderzoek bij Digikoppeling. Deze komen waarschijnlijk in het najaar.</p> <p>TO DK 19 april 2018: Logius heeft onderzoek gestart. Problemen worden geïnventariseerd, er wordt documentatie en broncode voor platformen (MS WCF) opgeleverd. Doorlooptijd 26 weken (najaar 2018).</p> <p>TO DK 1 november 2018: Logius heeft onderzoek rond interoperabiliteitsproblemen binnen WUS 2W-BE-S afgerond en heeft het conceptrapport met de leden gedeeld. Het onderzoek heeft aangetoond dat het Digikoppeling 2W-be-S profiel interoperabel is bij koppelingen tussen Java (Apache CXF) en Microsoft WCF platformen. Wel zijn er een aantal aanscherpingen voorgesteld voor het Digikoppeling WUS koppelvlak. Het wijzigingsvoorstel om de WSA:To in de respons optioneel te maken heeft de grootste impact op Edukoppeling. Het is wenselijk om in de EK Transactiestandaard op te nemen dat deze header bij EK verplicht is (zie issue #37). De resultaten van het onderzoek worden in de Edukoppeling WG van november besproken.</p> <p><u>Besluit:</u></p> <p>Wergroep 13 februari 2019: Het onderzoek van Logius geeft aan dat er bij het ondertekenen (2W-be-S) geen interoperabiliteitsprobleem is. Voor partijen die op .Net ontwikkelen wordt er door DUO code beschikbaar</p>	op standaard)				
--	--	---------------	--	--	--	--

		gesteld. Ondertekenen vraagt extra kennis, maar er is geen issue t.a.v. de standaard. Voorlopig wordt aangenomen dat partijen die op het .Net platform ontwikkelen een implementatie kunnen realiseren op basis van de reeds beschikbare documentatie en de code van DUO. Daarnaast wordt verwacht dat ook experts zich zullen registreren op het discussieplatform zodat zij partijen kunnen adviseren mochten er toch problemen zijn. Issue wordt afgesloten.					
6	DUO	<p>Transactiestandaard: 3.5 Foutafhandeling: WSA headers ontbreken in voorbeeld foutbericht</p> <p>De foutberichten zijn zoals Edukoppeling aangeeft 'normale' replyberichten. De wsa: attributes worden nu echter niet goed gevuld, en het voorbeeld in de Edukoppelingstandaard bevat zelfs helemaal geen wsa-attributes in de SOAP-header.</p> <p><u>Voorstel:</u></p> <p>SOAP-Fault voorbeeld aanpassen mbt WSA in de SOAP-header. Velden worden gevuld als een normale reply dus dat hoeft niet expliciet aangegeven te worden. Wel is het handig om in de foutafhandeling nog even aan te geven dat het om een normaal replybericht gaat waardoor de eisen die gelden voor een reply-bericht ook gelden voor een fault-bericht. De action property moet overigens wel specifiek gevuld worden met een default waarde: http://www.w3.org/2005/08/addressing/fault</p> <p><u>Besluit:</u></p> <p>Verwerken in versie 1.2.1</p>	Goedgekeurd Release 1.2.1	Midden	Laag	Laag	1
7	DUO	<p>Transactiestandaard: Paragraaf 3.4 Identificatie via WS-addressing header: WSA:MessageID / WSA:RelatesTo</p> <p>In de tabel staat 'eigen waarde'. Dit is onduidelijk. En omdat in één tabel zowel voor request als response 'eigen waarde' staat, kan dit impliceren dat het om dezelfde inhoud moet gaan. Bij relatesTo geldt dat dit veld functioneel alleen zin heeft als het relateert aan een message anders dan het bijbehorende requestbericht. Ook dit is niet duidelijk beschreven.</p> <p><u>Voorstel:</u></p> <p>Tekst bij request wijzigen in "Unieke waarde die dit requestbericht identificeert. Wordt door client bepaald"</p>	Goedgekeurd Release 1.2.1	Laag	Laag	Laag	1

		<p>Tekst bij respons wijzigen in "Unieke waarde die dit responsebericht identificeert. Wordt door service bepaald"</p> <p>Tekstuele wijzigingen die geen impact hebben op standaard verwerken.</p> <p>Besluit:</p> <p>Verwerken in versie 1.2.1</p>					
9	DUO	<p>Edukoppeling: Versioning</p> <p>De nieuwe architectuur van edukoppeling stelt alle partijen in staat services te leveren. Dat betekent dat iedereen ook te maken krijgt met het omgaan met meerdere versies. Omdat dit een ingewikkeld fenomeen is is het verstandig om dit daar waar mogelijk te standaardiseren. In de huidige versie van Edukoppeling is hier geen aandacht aan besteed. Concrete vragen: kan van alle partijen in de keten gevraagd worden om (tijdelijk) meerdere versies tegelijk te hosten? Welke versioneringsnummer strategie gaan we gebruiken (subminor, minr, major) en wat doet dit met de routing? Waar wordt vastgelegd wie welke versie vanaf wanneer host?</p> <p>Voorstel:</p> <p>Aanvullende documentatie opstellen (releasemanagment).</p> <p>Opnemen als actiepoint en issue sluiten.</p> <p>Besluit:</p> <p>Er is een releasemanagment document opgesteld. Hierin is reeds een eerste aanzet gedaan hoe hiermee om te gaan maar vereist op dit onderdeel nog verdere bespreking en uitwerking.</p> <p>Werkgroep 16 mei 2018: Inventarisatieverzoek bij leveranciers. Eind 2018 terugkoppeling /onderzoek en voorstel</p> <p>Werkgroep 10 oktober 2018: Nog geen voorderingen. Mogelijk komen er met de ontwikkeling van het OSR best practices rond versioning.</p>	Uitgewerkt in Best practice versie 0.9	Midden	Midden	Laag	1
11	Edustandaard	Begrippen in Architectuur en Transactiestandaard	Goedgekeurd	Midden	Laag	Laag	1

		<p>Momenteel zijn in het Architectuurdocument en de Transactiestandaard relevante begrippen opgenomen. Er komen meer en meer documenten en het is beheertechnisch niet wenselijk overal begrippen te onderhouden.</p> <p>Voorstel:</p> <p>Een extra document opstellen met alle relevante begrippen Hiermee worden de bestaande begrippenlijsten uit de Transactiestandaard en Architectuur verwijderd. Er is reeds een begrippenlijst met definities bij DUO beschikbaar waarvan de begrippen in het beoogde document opgenomen kunnen worden.</p> <p>Besluit:</p> <p>Voorstel wordt overgenomen. Verwijderen begrippen worden uit transactiestandaard/architectuur verwijderd. Verwerken in versie 1.2.1</p>	Release 1.2.1				
12	Edustandaard	<p>Verwijzing naar Digikoppeling standaard aanscherpen</p> <p>In de documenten verwijzen we naar Digikoppeling 3.0 maar niet naar de documentversies.</p> <p>In Edukoppeling 1.1 werd verwezen naar documentversie 2.6.2 (3 mei 2013), hierin wordt bijvoorbeeld nog SHA1 toegestaan.</p> <p>Voorstel:</p> <p>De Edukoppeling documentatie aanpassen en daar waar naar Digikoppeling verwezen wordt expliciet aangeven of we:</p> <ol style="list-style-type: none"> 1. Transparant meebewegen met Digikoppeling en dit wordt ook expliciet zo in documentatie vermeld, er wordt niet een verwijzing naar de Digikoppeling documentversie opgenomen. Er wordt altijd naar de vigerende Digikoppeling versie verwezen (die op logius site vermeld staan, deze is altijd de basis voor Edukoppeling. De werkgroep zorgt er voor dat de in beheer zijnde Edukoppeling versies hiermee in lijn zijn. 2. of we refereren naar een specifiek Digikoppeling WUS documentversie (nu versie 3.4 van 26 mei 2016). Een nieuwe versie van het WUS document heeft een nieuwe versie van Edukoppeling tot gevolg. 	Goedgekeurd Release 1.2.1	Midden	Laag	Laag	1

		<p>Besluit:</p> <p>In de Edukoppeling documentatie verwijzen we altijd naar de vigerende versie van Digikoppeling (https://www.logius.nl/standaarden/digikoppeling/architectuur-en-koppelvlakstandaarden/). Edukoppeling verwijst dus niet naar een specifieke versie van een Digikoppeling document. De Edukoppeling documentatie beschrijft hoe hiermee omgegaan wordt. Het voorstel is nu om een apart document op te stellen welke het releasemanagement toelicht (issue #14).</p> <p>NOTE: hoewel bovenstaande besluit bij overleg WG is genomen zijn we bij uitwerking toch tegen wat problemen aangelopen. Het betreft het volgende:</p> <ol style="list-style-type: none"> 1. Het zwevend volgen wordt lastig als er meerdere versie van EK zijn, zij verwijzen dan beide naar Logius site en het is niet inzichtelijk hoe een de vorige versie van EK was samengesteld (Logius heeft op site altijd de vigerende docset staan. Het formeel vastleggen van alle onderliggende standaarden in het voorschriftenoverzicht is niet wenselijk op langere termijn. Dit was een tijdelijke actie om aan vraag naar een overzicht te voldoen. Op termijn gaat Logius de docu rond DK verbeteren en is naar verwachting dit overzicht niet meer nodig. Het is ook onwenselijk omdat dit feitelijk dubbel beheer van DK specificatie is. 2. Logius is een wijzigingsvoorstel aan het uitwerken waarbij er geen hoofdversie meer gehanteerd wordt maar alleen nog met documentversies. We kunnen dan dus niet meer naar DK 3 verwijzen maar moeten naar specifieke docs (WUS/beveiliging/etc) verwijzen. Verder wordt zoals bekend DK 3 ingetrokken, dit leidt er toe dat er een nieuwe WUS 2.x versie opgesteld moet worden waarvan nog geen planning is. Bij TO DK werd onderkent dat er wel een overkoepelend beschrijvend document moet komen, een WUS bundel. Deze kan dus ook heel goed door Edukoppeling gebruikt worden als die er eenmaal is. <p>Gezien deze zaken nu nog in beweging zijn wordt voorlopig vanuit Edustandaard een Digikoppeling WUS bundel gedocumenteerd. Deze zal nog verwijzingen naar DK 3.0 documenten bevatten. Als Logius de eigen WUS bundel oplevert zal deze besproken worden om impact te bepalen en of naar dit document overgestapt kan worden.</p>					
--	--	--	--	--	--	--	--

13	Werkgroep	<p>Opnemen van uitleg rond toepassen van mustunderstand bij WSA headers in best practices</p> <p>Een verplichte WS-Addressing header bevat logischerwijs een mustunderstand attribuut met waarde "1", maar dit zit te diep in onderliggende standaarden beschreven. Dit soort zaken moeten in best practices toegelicht worden.</p> <p>Voorstel:</p> <p>Hoe bij verschillende WSA headers met het mustunderstand attribuut omgegaan moet worden, wordt opgenomen in Best Practice. Daar waar info ontbreekt moet echter door keten/werkgroep aangegeven worden.</p> <p>Besluit:</p> <p>WSA-Addressing mustunderstand attribuut wordt opgenomen in best practice document versie 0.2.</p>	Goedgekeurd	Midden	Laag	Laag	1
14	Werkgroep	<p>Releasemanagement toelichten.</p> <p>Naast het issue rond de relatie met Digikoppeling versie (#12) is er momenteel nog niet beschreven hoe er met de verschillen (onderliggende) standaarden omgegaan wordt, of wat het proces is mochten deze of Edukoppeling zelf wijzigen.</p> <p>Voorstel:</p> <p>Releasemanagement documenteren waar ondermeer de volgende zaken aan bod komen:</p> <ul style="list-style-type: none"> a. Verwijzen niet naar specifieke Digikoppeling versie, maar altijd naar vigerende algemene versie (issue #12). De werkgroep heeft de verantwoordelijkheid de Edukoppeling standaard in lijn te houden, een project geeft in PvE mogelijk wel expliciete versies aan. b. Als Edustandaard werkgroep gaan we niet over de implementaties en welke versie hierbij gebruikt moet worden. De keten streeft wel naar een minimaal aantal versies. Vanuit werkgroep wordt aangegeven welke in gebruik/ ondersteund worden. Het advies aan keten is om hier in te volgen. Deelnemers aan werkgroep moeten hier in het releasebeleid er 	Goedgekeurd	Midden	Laag	Laag	1

		<p>op sturen dat zaken niet te ver uit elkaar lopen.</p> <p>c. Logius moet ondersteunen dat er een landingspagina is voor de Digikoppeling hoofdversie, er wordt vanuit Edukoppeling niet naar specifieke (WUS) documentversies verwezen.</p> <p>d. Beschrijven wat relaties is tussen issues uit de issuelijst en de resulterende nieuwe release.</p> <p>Besluit:</p> <p>Er wordt een releasemanagementdocument opgesteld. Hierin is ook punt #9 verwerkt maar deze vraagt nog verdere bespreking en uitwerking</p>					
8	DUO	<p>Digikoppeling:Poort 443 is de standaard poort voor HTTPS verkeer.</p> <p>Digikoppeling heeft deze standaardwaarde verheven als verplicht te hanteren poort. Binnen Edukoppeling is het erg lastig om 443 af te dwingen. Ketenpartijen en DUO definiëren specifieke ranges en het blijkt bij meervoudige koppelingen juist erg onhandig om te standaardiseren op 443.</p> <p>DUO: standaardiseren op 443 is onhandig voor Edukoppeling. Voorstel is om dit vrij te laten net als de hostname (die immers ook vrij configureerbaar is). SaaS-leveranciers en grote partijen zoals DUO krijgen hierdoor meer vrijheid in de inrichting van hun netwerkconfiguratie</p> <p>BES: Dit is ook bij het TO Digikoppeling ter sprake gekomen. Daar zien alle betrokken partijen voordeel in het standaardiseren op portnummer en Digikoppeling blijft dit voorschrift ook handhaven.</p> <p>Voorstel:</p> <p>Het loslaten van dit voorschrift heeft ook impact op de benodigde logistieke keteninformatie. Het portnummer MOET dan als onderdeel van endpoint informatie beschikbaar zijn. Als onderdeel van actiepunten 49 wordt er gewerkt aan een nieuwe edukoppeling voorschrift die het gebruik van poortnummers vrij laat. We kijken hiermee af van Digikoppeling.</p>	Goedgekeurd	Midden	Midden	Midden	3-4

		<p>Besluit(dec 2016):</p> <p>Onder actiepoint 49 besproken. Er wordt gewacht op de notitie die in het kader van dit actiepoint opgesteld wordt. Naar verwachting zal er na bespreking van deze notitie een voorschriftwijziging doorgevoerd moeten worden. Issue blijft tot hier een besluit over is genomen open.</p> <p>WG 14 maart 2018: Wijzigingsvoorstel besproken en geaccepteerd. Wijziging kan mee in volgende medior release. Impact wordt als medior geclassificeerd omdat partijen in theorie andere poorten dan 443 kunnen gebruiken en dit voor de infrastructuur en communicatie van de endpoints impact heeft. In praktijk wordt voor meeste partijen geen impact verwacht omdat ketens nu al andere poorten dan 443 gebruiken en hierbij vooruit lopen op de standaard.</p>					
10	Edustandaard	<p>Transactiestandaard WS-Addressing versie</p> <p>Digikoppeling heeft voorschrift rond toe te passen WS-Addressing versie aangepast. Voor WS-Addressing konden twee versies gebruikt worden, de versie van 2005/08 (http://www.w3.org/TR/2005/CR-ws-addr-core-20050817/) of van 2006/05 (http://www.w3.org/TR/wsaddr-core/). Dit is echter in de release van mei dit jaar van Digikoppeling WUS aangepast. Hier wordt nu enkel de 2006/05 (http://www.w3.org/TR/wsaddr-core/) versie voorgeschreven.</p> <p>Voorstel:</p> <p>Dit is ook vorige keer bij Digikoppeling 3.0 toegelicht. In theorie is de impact gering omdat de nieuwe versie dezelfde namespaces voor attributen gebruikt. Wat het in praktijk betekend is nu nog onduidelijk. Het voorstel is om bij implementaties opmerkzaam te zijn welke WSA versie het platform ondersteund. We kunnen zo bijvoorbeeld in best practices inzichtelijk maken hoe verschillende platformen/tooling hiermee omgaan (ondersteunen allen 2006/05).</p> <p>Besluit (dec 2016):</p> <p>Issue blijft open omdat dit mogelijk grotere impact heeft dan nu verwacht wordt. Bij een volgende major/medior release wordt de standaard op dit punt aangepast. Tegen die tijd hebben we ook inzichtelijk hoe tooling/platformen hiermee omgaan.</p>	Goedgekeurd	Midden	Laag	Laag	2

		<p>Wijziging kan mee in volgende release als dit naar verwachting geen issue opleverd, is dit getest door partijen?</p> <p>Werkgroep 16 mei 2018: Refereren naar DigiKoppeling release notes. Edukoppeling hoeft op dit punt niet aangepast worden, maar de wijziging in Digikoppeling wordt wel ook in Edukoppeling release notes benoemd.</p>					
15	Edustandaard	<p>Gebruik ODOC certificaten</p> <p>Het 3^e voorschrift van de transactiestandaard stelt dat het gebruik van PKI-ODOC en PKI-Overheid certificaten toegestaan is. Binnen de OSO keten is de vraag naar voren gekomen of het toestaan van ODOC certificaten handig is, dit lijkt partijen extra inspanning te vragen, onder anderen doordat PKIoverheid certificaten standaard in truststores van verschillende platformen zitten, dit geldt niet voor ODOC certificaten.</p> <p>Voorstel:</p> <p>Er is besloten om deze problematiek vast te leggen in het verslag en verder te onderzoeken en nader te beschrijven in een notitie. Op basis van de notitie wordt er na consultatie in andere gremia besloten of er uiteindelijke wordt overgegaan tot het opstellen van een RFC.</p> <p>Kunnen ODOC certificaten bij een Edukoppeling koppelvlak gebruikt worden of te wel moeten we het voorschrift met de mogelijkheid om ODOC certificaten te gebruiken handhaven?</p> <p>Besluit:</p> <p>Werkgroep 16 mei 2018: De notitie is opgesteld en besproken. ODOC cert worden in IAA context gebruikt (PO). Verder mogelijk in test trajecten. Het voorstel om de Transactiestandaard aan te passen en ODOC certificaten te verwijderen wordt geaccepteerd. ODOC certificaten worden in Edukoppeling (SaaS model) niet meer gebruikt worden. Hiermee wordt alleen het gebruik van PKIoverheid certificaten toegestaan.</p>	Goedgekeurd	Midden	Midden	Midden	3
16	DUO	<p>Aanpassing foutafhandeling</p> <p>In 1.2 zijn een aantal foutcodes gestandaardiseerd. In Digikoppeling zijn deze opgenomen in de best-practices, in Edukoppeling als verplicht in de transactiestandaard. Niet alle fouten zijn echter simpel op te sporen en komen nauwelijks voor. De vraag: is het verplicht op alle situaties ter controleren of niet (optioneel).</p>	Afvoeren	Midden	Laag	Laag	2

		<p>Voorstel:</p> <p>Een voorstel wordt door DUO uitgewerkt.</p> <p>Ook Digikoppeling is in beweging op dit punt. Digikoppeling zal de foutcodes in bestpractice opnemen. Wanneer deze er zijn is nu nog onbekend. Er is in ieder geval afgesproken dat de 1.2.1 versie geen impact mag hebben op foutcodes. De komende periode gaan we besluiten hoe en waar foutafhandeling definitief een plek krijgt.</p> <p>Behouden we de huidige voorschriften rond foutcodes? Deze moeten door services geïmplementeerd worden of zijn het best practices waar een web service de keuze heeft om dit wel of niet te doen.</p> <p>Werkgroep 16 mei 2018: Handhaven huidige situatie, foutcodes blijven in transactiestandaard staan. Foutmeldingen moeten client helpen en is het handig om dit verplicht te stellen. Services moeten dit dus implementeren en testen.</p>					
17	DUO	<p>Vulling WSA:To in request</p> <p>De WSA:To in het request bevat een wsdl-adres. Dit is een overblijfsel uit 1.1 om ervoor te zorgen dat dit veld compatibel blijft met 1.1. In DK wordt dit veld anders gebruikt, in Edukoppeling lijkt eigenlijk alleen het OIN belangrijk. Is het dan niet veel simpeler en duidelijker dat we hier ook anonymous verplicht stellen?</p> <p>Voorstel:</p> <p>Verwerken in volgende medior of major release.</p> <p>Overweging: toets hoe toolkits hiermee omgaan, vullen deze standaard de wsa:to met WSDL endpoint?</p> <p>Besluit:</p> <p>Bespreking 24 januari: Bij DK WUS zal het OIN waarschijnlijk optioneel in de WSA To en From header opgenomen worden. Willen we het WSA:To veld in EK dan nog steeds vullen met anonymous of aansluiten op de verwachte generieke vulling van DK die hierin waarschijnlijk het endpoint van de web service opneemt? BKWI gaat hier ook anders mee om.</p> <p>Werkgroep 16 mei 2018: Toelichten hoe BKWI hiermee omgaat. Op basis</p>	Afvoeren	Midden	Midden	Midden	2

		<p>daarvan besluit nemen.</p> <p>Bespreking 4 juli 2018: Er wordt besloten het issue af te voeren. 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.</p>					
18	WG	<p>Foutcodes opnemen indien WS-A headers ReplyTo of FaultTo in bericht zijn opgenomen.</p> <p>Voorstel:</p> <p>In de tabel 3.4 Identificatie via WS-addressing header staat nu "WSA:ReplyTo: Wordt niet gebruikt". Partijen interpreteren dit dat het een keuze is of ReplyTo wel of niet opgenomen kan worden in request. Het voorschrift moet eenduidiger. Tekst voor zowel ReplyTo als FaultTo wijzigen in "Mag niet voorkomen"De volgende foutcodes toevoegen:</p> <ul style="list-style-type: none"> • #XX "WSA:ReplyTo mag niet voorkomen" • #XX "WSA:FaultTo mag niet voorkomen" <p>Besluit:</p> <p>Werkgroep 16 mei 2018: Deze velden mogen in de nieuwe release toegepast worden (zie issue #26). Hiermee zijn deze foutmeldingen niet meer relevant. Issue wordt afgevoerd.</p>	Afvoeren	Laag	Laag	Midden	2
19	Johan Geerts / Robert Kars (DUO)	<p>Transactiestandaard voorbeeld foutbericht (figuur 4).</p> <p>Het foutbericht bevat nu een vulling die door bepaalde client-implementaties niet goed verwerkt kunnen worden. Binnen het soap:Fault element worden de elementen Value en Tekst voorzien van een qualifier.</p> <p>WS0-I BP1.2: R1001: "When an ENVELOPE is a Fault, the element children of the soap:Fault element MUST be unqualified."</p> <pre><soap:Fault> <soap:Faultcode> <soap:Value>soap:Client.DK0002</soap:Value> </soap:Faultcode> <soap:Faultstring> <soap:Text xml:lang="nl">...</soap:Text ></pre>	Goedgekeurd	Midden	Laag	Midden	2

		<pre></soap:Faultstring> </soap:Fault></pre> <p>Voorstel:</p> <p>Voorbeeld op bovenstaande aanpassen.</p> <p>Er zitten nog andere fouten in het voorbeeld die gewijzigd worden:</p> <ol style="list-style-type: none"> 1. Inconsistent gebruik van prefix soap en soapenv (soap:Header tbv WSA headers) 2. Tekst binnen soap.Fault unquaified maken. 3. Verwijderen van Edukoppeling code in Faultcode (<Faultcode> soap:Client.DK0002). WS-I BP 1.2: R1031: Faultcode: SHOULD NOT use of the SOAP 1.1 "dot" notation to refine the meaning of the fault). In faultcode met koppelteken werken (soap: Client-DK0002) of indien niet werkbaar in de Faultstring ook code opnemen. <p>Besluit:</p> <p>Het voorbeeld aanpassen op punten 1 & 2. Voor het derde punt geeft WS-I aan dat het gewenst is niet een dot notatie toe te passen. Omdat dit nu al toegepast wordt en geen problemen heeft opgeleverd wordt het voorbeeld op dit punt niet aangepast. Bij GAB / Digikoppeling loopt nog een onderzoek of dot-notitie wenselijk is.</p> <pre><soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" > <soap:Header xmlns:wsa="http://www.w3.org/2005/08/addressing"> ... <soap:Fault> <faultcode>soap:Client.DK0002 </faultcode> < faultstring>Niet geautoriseerd OIN</faultstring> </soap:Fault></pre> <p>Werkgroep 16 mei 2018: Voorstel wordt geodgerkeurd en kan meegenomen worden in de volgende versie. Of hierbij de dot-notatie of een koppelteken gebruikt wordt moet nog wel besloten worden. De keuze bij GAB (Gemeenschappelijke Afspraken Berichten) is nog niet gemaakt.</p>					
--	--	--	--	--	--	--	--

20	Kennisnet	<p>Voorschriften rond vulling OIN</p> <p>Momenteel ontbreekt er een voorschrift hoe OIN gevuld moet worden. Het formaat is <prefix><nummer><suffix>, het totaal is 20 karakters en de prefix 8. In het identificatie en authenticatie document van Digikoppeling wordt aangegeven dat het BRIN gebruikt wordt, maar er wordt niet beschreven hoe de overige 12 karakters over BRIN en suffix verdeeld moeten worden. Ook is wellicht van belang om hier impact van RIO in mee te nemen</p> <p>Voorstel:</p> <p>In identificatie en authenticatie document is het volgende opgenomen: '0000007'(prefix) + de BRIN (3 voorloophullende, BRIN = 4 posities + 00, hoofdnummer) + het administratienummer (3 posities, suffix)</p> <p>Besluit:</p> <p>Werkgroep 16 mei 2018: In het Identificatie en authenticatie document is nu de expliciete vulling opgenomen (versie 12 maart 2018).</p>	Goedgekeurd	Hoog	Laag	Midden	2
21	SBB	<p>Controle door client van CN in het certificaat en de hostnaam van de service.</p> <p>Voorstel:</p> <p>Vaststellen hoe hiermee om te gaan en mogelijk aanvullende info opstellen op basis van Edukoppeling implementaties. Punt is ook bij Digikoppeling aangegeven. Er is nu geen uitputtende lijst met maatregelen hoe een bepaald betrouwbaarheidsniveau gehaald kan worden.</p> <p>Besluit:</p> <p>Werkgroep 16 mei 2018: Dit onderwerp is bij agendapunt 4 besproken. Het probleem treedt op als er een verschil is tussen de CN in het certificaat en de (hostnaam van de) naam van de service. Partijen passen verschillende manieren toe om services te combineren achter een certificaat. 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.</p> <p>Werkgroep 4 juli 2018: Navraag heeft opgeleverd dat er geen</p>	Goedgekeurd	Midden	Laag	Midden	1-2

		interoperabiliteitsproblemen zijn bij het toepassen van SAN certificaten en deze kunnen dus toegepast worden. Het toepassen hiervan wordt toegelicht in het Best Practices document.					
22	OSO	<p>Beveiligingsvoorschriften ciphersuites</p> <p>Er worden door Digikoppeling ciphers toegestaan die geen gebruik maken van Perfect Forward Secrecy. OSO staat het gebruik van deze ciphers niet toe. Bronnen hiervoor zijn de cipher lijst die Mozilla samen heeft gesteld voor modern compatibility: https://wiki.mozilla.org/Security/Server_Side_TLS#Modern_compatibility, alsmede het researchwerk van Qualys die oa de gerenomeerde SSLTEST hebben gebouwd, hun documentatie staat op: https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices.</p> <p>Voorstel:</p> <p>OSO past geen Edukoppeling toe en hiermee speelt dit issue breder dan enkel de Edukoppeling standaard. Eerder is de behoefte voor een onderwijsbeveiligingsplatform besproken (ook met de IBP werkgroep). Destijds is besloten om voorlopig de overheidsbronnen (zoals Digikoppeling en NCSC te volgen).</p> <p>Met IBP WG bespreken of we toch iets centraal voor het onderwijs geregeld zou moeten worden om te voorkomen dat in de toekomst in verschillende ketens wedermaal verschillende keuzes gemaakt worden.</p> <p>TO DK 19 april 2018: Logius gaat namens TO DK nog eens navraag doen bij NCSC over het proces. Daarbij moet er niet alleen gekeken worden naar ciphers die uitgefaseerd moeten worden (voldoen volgens TO DK niet meer), maar ook naar ciphers die gaan komen (TLS 1.3).</p> <p>Werkgroep 16 mei 2018: Dit onderwerp is als onderdeel van agendapunt 3 besproken. Vanuit TO Digikoppeling is ondertussen vernomen 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). Het onderwijsdomein moet bepalen of deze volledig overgenomen kan worden of dat we een eigen lijst voor het onderwijs moeten gaan voorschrijven. We volgen de ontwikkelingen bij Digikoppeling.</p> <p>EK WG 10-10-2018: Er wordt nog met de IBP WG gesproken om S2S beveiligingsvoorschriften voor het onderwijsdomein op te stellen. Issue</p>	Goedgekeurd en uitgevoerd door werkgroep UBV. Heeft wel impact op EK docs	Hoog	Midden	Midden	3

		blijft open (is geen onderdeel van versie 1.3). Besluit: Werkgroep 18 maart 2020: Goedgekeurd en uitgevoerd door werkgroep UBV. Heeft wel impact op EK docs					
24	Edustandaard	Digikoppeling 3.0 is vervallen, er moet worden verwezen naar specifieke Digikoppeling documenten Voorstel: Alle verwijzingen naar DK 3.0 uit documentatie verwijderen. Controleren release notes van nieuwe DK documentatie op mogelijke wijzigingen met impact. Opnemen van verwijzing naar het Digikoppeling overzicht actuele documentatie en compliance document. https://www.logius.nl/fileadmin/logius/ns/diensten/digikoppeling/digikoppeling_2.0/Digikoppeling_Overzicht_Actuele_Documentatie_en_Compliance_v1.0.pdf Besluit: Alle verwijzingen worden vervangen met een verwijzing naar het Digikoppeling "Overzicht actuele documentatie en compliance" document.	Goedgekeurd 1.3	Midden	Laag	Laag	1
25	Kennisnet	Verduidelijken 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. 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. Voorstel: 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	Goedgekeurd 1.3	Midden	Laag	Laag	3

		<p>geen oin-parameter zou moeten bevatten.</p> <p>Besluit:</p> <p>Werkgroep 16 mei 2018: Aanbeveling 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.</p>					
26	Kennisnet	<p>ReplyTo en FaultTo mogen in request opgenomen worden</p> <p>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 wsa-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.</p> <p>Voorstel:</p> <p>Overweeg het verbod op faultTo op te heffen en documenteer het gebruik ervan in situaties met routing via intermediairs</p> <p>Besluit:</p> <p>Werkgroep 16 mei 2018: Aanbeveling wordt overgenomen. De toe te passen WSA headers in het request en response bericht worden overgenomen van de Digikoppeling tabel.</p>	Goedgekeurd 1.3	Midden	Laag	Laag	3
27	Edustandaard	<p>Architectuurdocument: verwijzing naar het certificeringsschema aanpassen</p> <p>Voorstel:</p> <p>Het architectuurdocument naar de verschillende documenten van het</p>	Goedgekeurd 1.3	Midden	Laag	Laag	1

		<p>certificeringsschema laten verwijzen.</p> <p>Besluit:</p> <p>Werkgroep 16 mei 2018: Akkoord met het voorstel.</p>					
28	Edustandaard	<p>Architectuurdocument: overzichtsplaat (figuur 11) aanpassen</p> <p>Voorstel:</p> <p>De overzichtsplaat (figuur 11) aanpassen. Het certificeringsschema wordt breder toegepast dan alleen Edukoppeling. Aangeven welke bouwstenen relevant zijn om end-to-end beveiliging te realiseren.</p> <p>Besluit:</p> <p>Werkgroep 16 mei 2018: In nieuw voorstel complexiteit van plaat reduceren.</p> <p>Werkgroep 4 juli 2018: Conceptplaat is goedgekeurd maar zal mogelijk nog wat in detail aangepast worden. Plaat wordt opgenomen in de 1.3 release.</p>	Goedgekeurd 1.3	Midden	Laag	Laag	1
29	Edustandaard	<p>Fijnmazige identificatie van diensten/afdelingen</p> <p>Private partijen hebben als basis voor het OIN het kvk nummer en de suffix hiervan is altijd "0000" (of "000" bij RSIN). Zij kunnen dus geen certificaten met een andere suffix gebruiken om afdelingen of diensten van een identiteit te voorzien. Verder kunnen zij ook geen gebruik maken van subOINs. Hoewel er nu geen urgentie is om fijnmazige identificatie toe te passen is het wel te verwachten dat dit op termijn gaat spelen. We willen de use cases en mogelijke alternatieven inventariseren.</p> <p>Voorstel:</p> <p>Of dit een probleem is binnen het onderwijs hangt deels af hoe formeel we dit willen regelen. Binnen OSO wordt er bijvoorbeeld nu gewerkt met een vrij in te voeren alfanumerieke karakterreeks waarmee een softwarepakket van een leverancier geïdentificeerd wordt.</p> <p>Bij de overheid worden er waarschijnlijk verschillende keuzes gemaakt omdat dit niet gestandaardiseerd is. Logius heeft een voorstel opgesteld voor het identificeren van (basis)registraties in het Digikoppeling domein.</p>	Afgevoerd	Laag	Laag	Laag	3

		<p>Hierbij wordt een URI strategie gehanteerd: <a href="https://digikoppeling.gdi.nl/<registerhouder>/<registratie-aanduiding->">https://digikoppeling.gdi.nl/<registerhouder>/<registratie-aanduiding-> https://digikoppeling.gdi.nl/Kadaster/BAG. De status van dit voorstel is nu nog onduidelijk. Het kadaster lijkt te kiezen voor https://baq.basisregistraties.overheid.nl/</p> <p>Besluit:</p> <p>EK WG 10-10-2018: Als een private partij een gateway gebruikt is de partij verantwoordelijk voor identificatie en routing. Er is geen behoefte aan aanvullende afspraken rond identificatie van voorzieningen binnen het onderwijs. Issue wordt afgevoerd.</p>					
30	Kennisnet VA	<p>Vulling WSA Action bij SoapFault</p> <p>Welke action moet er worden teruggegeven worden als het om een SoapFault gaat? In het voorbeeld staat 'http://www.w3.org/2005/08/addressing/soap/fault', in de documentatie staat 'http://www.w3.org/2005/08/addressing/fault'. Beide zijn valide dus wat moet gebruikt worden?</p> <p>WS Addressing (http://www.w3.org/TR/ws-addr-soap/) stelt:</p> <ol style="list-style-type: none"> 1. http://www.w3.org/2005/08/addressing/fault: This action SHOULD NOT be used as an action value in messages other than those carrying WS-Addressing faults. SOAP modules, extensions and applications SHOULD define custom [action] values for the faults they describe but MAY designate use of the following [action] value instead: 2. http://www.w3.org/2005/08/addressing/soap/fault: The [action] value SHOULD be used for SOAP defined faults including version mismatch, must understand, and data encoding unknown (data encoding unknown is onderdeel SOAP1.2 Fault Subcode). <p>Voorstel:</p> <p>[http://www.w3.org/2005/08/addressing/fault] gebruiken als het om WS Addressing fouten gaat (foutcodes codes 5, 6, 7, 8, 20, 21, 22).</p> <p>[http://www.w3.org/2005/08/addressing/soap/fault] gebruiken als het om version mismatch en must understand fouten gaat.</p> <p>Bij implementaties kan overwogen worden om de</p>	Uitgewerkt in Best practice versie 0.9	Midden	Laag	Laag	1

		<p>http://www.w3.org/2005/08/addressing/soap/fault voor overige SOAP Fault berichten te gebruiken. Het kan echter wenselijk zijn dat men in de WSA:Action van de SOAP Fault de wsa:action van de WSDL/operatie opneemt. Wat leidend bij deze keuze is hoe de SOAP toolkits hiermee omgaan. De werkgroep heeft hier momenteel geen informatie over.</p> <p>Besluit:</p> <p>EK WG 10-10-2018: Voorstel onderdeel Best practices versie 1.0. Oplevering BP 1.0 gepland voor Q1 2019.</p>					
31	Kennisnet VA	<p>Request zonder WSA From of zonder OIN (fout 20 of 21)</p> <p>Zonder WSA:From in request is het OIN voor de respons niet bekend. Wat moet er dan worden teruggestuurd en naar wie? Conform foutafhandeling zal er een SoapFault (fout 20 of 21) gestuurd worden. Maar de WSA To kan niet gevuld worden omdat deze niet bekend is..</p> <p>Voorstel:</p> <p>Dit scenario moet bij foutafhandeling best practices worden beschreven. Als in WSA:From van een request een OIN ontbreekt dan foutmelding als response sturen waarin het OIN in de WSA:To leeg is. De verwachting is dat dit alleen voorkomt in de testfase, in die situatie is het acceptabel om invalide respons te sturen (zonder vulling van OIN bij WSA:To).</p> <p>Besluit:</p> <p>EK WG 10-10-2018: Onderdeel Best practices versie 1.0. Oplevering BP 1.0 gepland voor Q1 2019.</p>	Uitgewerkt in Best practice versie 0.9	Midden	Laag	Laag	1
32	Kennisnet VA	<p>Request bevat header dat geen onderdeel is van een Edukoppeling profiel. Wat moet er dan worden teruggestuurd.</p> <p>Voorstel:</p> <p>Voor deze situatie is foutcode 10 (Andere headers) gedefinieerd en wordt verondersteld dat er SOAP fault wordt teruggestuurd. De verwachting is overigens dat dit soort fouten alleen in de testfase voorkomen.</p> <p>In best practice documenteren hoe hiermee omgegaan moet worden. Vereisen we vanuit standaard dat het request niet verwerkt mag worden</p>	Uitgewerkt in Best practice versie 0.9	Midden	Laag	Laag	1

		<p>en een foutbericht gestuurd moet worden?</p> <p>Besluit:</p> <p>EK WG 10-10-2018: Onderdeel Best practices versie 1.0. Oplevering BP 1.0 gepland voor Q1 2019.</p>					
33	Kennisnet VA	<p>Validatie van waardes in WSA headers</p> <p>Er is niet duidelijk uit de documentatie te herleiden in hoeverre de waardes van headers moeten worden gevalideerd. Moeten er ook validaties worden doorgevoerd zoals uuid validatie op MessageID en url validatie op From en To en mogelijk nog meer?</p> <p>Voorstel:</p> <p>In de Edukoppeling architectuur worden 5 typen fouten onderscheiden: (1) Syntaxfouten, (2) Service gesloten, (3) Service reageert niet (tijdig), (4) Functionele fouten, (5) Prestatie-fouten.</p> <p>Deze vraag gaat over fouttype (1) - fouten in de syntax van het bericht. Voor fouttypen (1) en (2) wordt verwezen naar de lijst in de transactiestandaard.</p> <p>Conform overige foutcodes wordt ook bij foutcode 11 impliciet verwacht dat er een SOAPFault gegeven wordt met foutcode 11.</p> <p>Vereisen we vanuit standaard dat het request niet verwerkt mag worden en een foutbericht gestuurd moet worden?</p> <p>Besluit:</p> <p>EK WG 10-10-2018: In Best practices versie 1.0. documenteren dat er een SOAPFault gegeven moet worden als type van het veld afwijkt van de standaard. Nieuw issue (#38): In Transactiestandaard bij foutcodes aangeven dat er gecontroleerd moet worden op voorgeschreven type van velden.</p> <p>WG 28 november 2018: Issue afvoeren (zie ook i#38), deze eisen volgen uit WSA standaard en partijen moeten hier zelf hun verantwoordelijkheid in nemen.</p>	Afgevoerd	Midden	Laag	Laag	1

34	Kennisnet VA	Validatie certificaat tegen Certificate Revocation List PKI Overheid	Uitgewerkt in Best practice versie 0.9	Midden	Laag	Laag	1
<p>Hoe wordt het certificaat in het bericht gevalideerd tegen de CRL? Hoe bepalen we welke CRL we moeten gebruiken en wat doen we als we de CRL(s) niet kunnen ophalen?</p> <p>Voorstel:</p> <p>De Edukoppeling transactiestandaard zegt hier zelf niets over, maar verwijst wel naar Digikoppeling. Digikoppeling zegt: "De geldigheid van het certificaat wordt getoetst met betrekking tot de geldigheidsdatum en de Certificate Revocation List (CRL) die voldoet aan de eisen van PKI-overheid" (https://www.logius.nl/fileadmin/logius/ns/diensten/pkioverheid/programma-van-eisen/02_2018/PvE_deel3_basiseisen_v4.6.pdf)</p> <p>De verantwoordelijkheid voor het beschikbaar zijn van een CRL ligt bij de TSP - de Trust Service Provider. (Digikoppeling: "De TSP dient CRL's uit te geven conform de eisen, die daaraan zijn gesteld in bijlage A van dit document, te weten "CRL- en OCSP-profielen".) Het certificaat zelf bevat de informatie die nodig is om de locatie van de CRL van de TSP te bepalen (CRL Distribution Point).</p> <p>De CRLs van de root certificate van PKIOverheid staan op https://crl.pkioverheid.nl/</p> <p>Vanuit het PvE van PKIOverheid zal naar alle waarschijnlijkheid vereist worden dat CRL's beschikbaar zijn. TSP's stellen periodiek een nieuwe CRL beschikbaar. De gebruikte software zal hier rekening mee moeten houden en is zowel relevant voor het TLS koppelvlak als bij ondertekende en/of versleutelde berichten.</p> <p>Opnemen in FAQ of Best Practices?</p> <p>Besluit:</p> <p>EK WG 10-10-2018: In Best practices versie 1.0. documenteren</p>							
35	Kennisnet VA	Validatie hiërarchie van certificaat. Hoe gaat de validatie van de hiërarchie van het certificaat in zijn werk?	Uitgewerkt in Best practice versie 0.9	Midden	Laag	Laag	1
<p>Dit is vaak standaard functionaliteit van systemen / bibliotheken die het werken met certificaten ondersteunen. De software biedt de mogelijkheid om in een truststore certificaten op te nemen. Hierin zijn over het</p>							

		<p>algemeen de certificaten (hierarchie publiek domein PKIo) van het publieke domein al standaard opgenomen.</p> <p>Voorstel:</p> <p>Opnemen in FAQ of Best Practices? Onderzoeken of hiërarchie op basis van private domein ook standaard opgenomen zijn, of dat hier wel extra handelingen voor vereist zijn.</p> <p>Besluit:</p> <p>EK WG 10-10-2018: Onderdeel Best practices versie 1.0 en FAQ. Functionele beschrijving, niet specifiek voor bepaalde platformen.</p>					
--	--	---	--	--	--	--	--

36	Kennisnet VA	<p>Waarom moet zowel request en respons ondertekend worden als de respons alleen een ontvangstbevestiging betreft?</p> <p>Bij overweging van WB011 staat: "Beveiligingseisen kunnen op het niveau van het bericht gedefinieerd worden, maar niet alle toolkits kunnen hiermee overweg. Totdat alle belangrijke toolkits dit wel kunnen, is het beter om bericht beveiliging op serviceniveau te definiëren".</p> <p>De vraag is of dit nog steeds geldt. Wellicht wat laat voor het onderzoek, maar is misschien wel een goed punt om eens opnieuw te toetsen?</p> <p>Besluit:</p> <p>Vraag uitgezet bij Logius: TO DK 1-11-2018: Alleen ondertekenen van req-of res wordt niet toegepast en niet ondersteund door tooling</p> <p>WG 28 november 2018: Mechanisme wordt nu overal toegepast, extra profielen met keuze voor signing op berichtniveau (ipv operatie) is onwenselijk en maakt de standaard onnodig complexer. Issue wordt afgevoerd.</p> <p>Er wordt aanvullend nog gesproken over hoe foutieve ondertekeningen verwerkt moeten worden. Met name bij een response met fouten rond ondertekening leveren onduidelijkheid op. Er wordt voorgesteld om dit bij AR te bespreken. Bij een response met fouten in ondertekening ziet de ontvanger het als een fout, de verzender weet echter niet dat het mis is gegaan. Er moet onderzocht worden of een foutieve ondertekening van</p>	Afvoeren	Laag	Laag	Laag	1
----	--------------	--	----------	------	------	------	---

		response afgekeurd moet worden en niet verwerkt mag worden, ook als het hier enkel om een technische terugmelding gaat dat het bericht is ontvangen? Robert en Herrie gaan dit onderzoeken (actiepunt #86)					
37	BES	<p>In WUS conceptversie 3.7 is de WSA:To in response optioneel gemaakt.</p> <p>Voorstel:</p> <p>Als de conceptversie WUS definitief wordt moet in de EK Transactiestandaard (tabel 1) aangegeven worden dat de WSA:To header verplicht is in de response.</p> <p>Besluit:</p> <p>WG 28 november 2018: Meenemen in versie 1.3</p>	Goedgekeurd Versie 1.3	Midden	Laag	Laag	3
38	BES	<p>Het is niet duidelijk of de waardes in headers moeten worden gevalideerd en SOAP Fault response moet worden gegeven als de waarde niet voldoet aan het voorgeschreven type.</p> <p>Moeten er ook validaties worden doorgevoerd zoals uuid validatie op MessageID en url validatie op From en To?</p> <p>Voorstel:</p> <p>In Transactiestandaard bij foutcodes aangeven dat er gecontroleerd moet worden op voorgeschreven type van velden</p> <p>Besluit:</p> <p>WG 28 november 2018: Issue afvoeren, deze eisen volgen uit WSA standaard en partijen moeten hier zelf hun verantwoordelijkheid in nemen.</p>	Afgevoerd	Laag	Laag	Midden	2
39	DUO	<p>Voeg architectuur paragraaf 4.5 (foutafhandeling) samen met paragraaf 3.8 van de transactiestandaard</p> <p>Besluit:</p>	Goedgekeurd Versie 1.3	Laag	Laag	Laag	1

		WG 28 november 2018: Akkoord met wijziging voor versie 1.3					
40	DUO	<p>Edukoppeling compliancevoorziening</p> <p>De voorziening van Logius dekt veel af wat ook voor Edukoppeling relevant is. Maar Edukoppeling heeft wel zo zijn eigen bijzonderheden. Het streefbeeld blijft een eigen compliancevoorziening of een module boven op die van Logius is, ook al is er nu geen concrete opdrachtgever die daarom vraagt.</p> <p>Besluit:</p> <p>WG 28 november 2018: Architectuur paragraaf 5.1 (figuur 11). Compliancevoorzieningen van Digikoppeling en Edukoppeling opnemen. Opmerking in tekst dat de compliancevoorziening voor Edukoppeling nog niet gerealiseerd is.</p>	Goedgekeurd Versie 1.3	Laag	Laag	Laag	1
41	DUO	<p>Architectuurdocument: Zijn er richtlijnen wanneer welke versie gebruikt wordt én kan je aan een wsdl of bericht zien welke versie het is?</p> <p>Voorstel</p> <p>Wat gebruikt moet worden hangt af van context en kan heel divers zijn. Hiervoor moet een BIV classificatie uitgevoerd worden. Dit kan mogelijk aangegeven in de documentatie van de WSDL. Verder zou onderzocht kunnen worden of WS-Policy een oplossing biedt. Het is wel waarschijnlijk dat verschillende platformen hier verschillend mee omgaan.</p> <p>Besluit:</p> <p>WG 28 november 2018: Issue registreren, maar is geen onderdeel van Architectuurdocument versie 1.2.2</p> <p>WG 13 februari 2019: Op contractniveau (documentation element in WSDL) kan aangegeven worden welke versie Edukoppeling toegepast wordt. Dit kan ook met WS-policy maar is complexer en kan bij client problemen geven. De stelling is dat dit (voorlopig) buiten de standaard valt. Partijen zijn vrij om hier invulling aan te geven, bijvoorbeeld door het opnemen hiervan in het Plan van Eisen. Issue afvoeren.</p>	Afgewezen	Midden	Midden	Midden	1-3

42	DUO	<p>Transactiestandaard: Optioneel toestaan van replyTo Header betekend niet dat Edukoppeling profielen asynchrone uitwisseling toestaan.</p> <p>De replyTo Header wordt in 1.3 optioneel toegestaan om praktische redenen en compliancy met Digikoppeling. Gegevensuitwisseling via een Edukoppeling profiel is altijd synchroon.</p> <p>Voorstel</p> <p>Er wordt een opmerking bij de tabel opgenomen dat een asynchrone uitwisseling niet ondersteund wordt. De replyTo header is optioneel om in lijn te zijn met Digikoppeling.</p> <p>Besluit:</p> <p>WG 28 november 2018: Issue registreren en in versie 1.3 verwerken.</p>	Goedgekeurd Versie 1.3	Laag	Laag	Laag	2			
43	DUO	<p>In de webservicewereld is het niet ongebruikelijk dat via de WSA:To de wsdl opgevraagd kan worden. Die vraag heeft DUO ook wel eens gehad. Deze wijziging suggereert dat dat kan. Het lijkt wel een goed idee, maar op dit moment doet DUO dat niet. Is dat ook de bedoeling van de wijziging. Of wordt het dat?</p> <p>Voorstel</p> <p>Bij het voorbeeld foutbericht (figuur 2) de note: /* het WSDL-adres */ verwijderd. De standaard schrijft niet voor dat een WSDL via de WSA:To header opgehaald kan worden.</p> <p>Besluit:</p> <p>WG 28 november 2018: Issue registreren en in versie 1.3 verwerken.</p>	Goedgekeurd Versie 1.3	Laag	Laag	Laag	2			
42 B	DUO	<p>Nieuwe foutcodes</p> <p>We missen nu EK0030, EK0031 en DK0050.</p> <p>Voorstel</p> <table border="1" data-bbox="421 1369 1200 1433"> <tr> <td>Client.EK0030*</td> <td>OIN in TLS certificaat</td> <td>De client moet de verbinding opzetten met een</td> </tr> </table>	Client.EK0030*	OIN in TLS certificaat	De client moet de verbinding opzetten met een	Goedgekeurd Verwerkt in concept in WUS 1.4	Midden	Laag	Laag	2
Client.EK0030*	OIN in TLS certificaat	De client moet de verbinding opzetten met een								

		<table border="1"> <tr> <td></td> <td>ontbreekt of is ongeldig</td> <td>digikoppeling compliant PKI-overheid certificaat.</td> </tr> <tr> <td>Client.EK0031</td> <td>Berichtondertekening niet aanwezig of onjuist</td> <td>Het bericht moet volgens contract ondertekend worden maar de ondertekening is ongeldig of niet aanwezig</td> </tr> <tr> <td>Server.EK0050*</td> <td>Service afhandeling geeft fout</td> <td>Het proces dat het serviceverzoek moet afhandelen geeft een fout</td> </tr> </table> <p>EK0030*: ik neem aan dat dit afgedwongen wordt op het TLS-endpoint. Dit bericht mag eigenlijk helemaal niet verder de interne keten in komen. Het is een fout op protocol niveau, niet op http niveau. Dat betekent dat je dit mogelijk (afhankelijk van je interne keuzes) helemaal niet als SOAP:Fault terug kan sturen. Naar nu blijkt gebeurt dat toch. In testtrajecten kan ik me dit wel voorstellen overigens en dan is zo'n foutcode wel handig</p> <p>EK0050*: In principe is dit een interne fout bij de serviceleverancier waar de client geen actie op kan ondernemen, anders dan signaleren.</p> <p>Besluit:</p> <p>WG 14 januari 2021: Verwerken in 1.4</p>		ontbreekt of is ongeldig	digikoppeling compliant PKI-overheid certificaat.	Client.EK0031	Berichtondertekening niet aanwezig of onjuist	Het bericht moet volgens contract ondertekend worden maar de ondertekening is ongeldig of niet aanwezig	Server.EK0050*	Service afhandeling geeft fout	Het proces dat het serviceverzoek moet afhandelen geeft een fout					
	ontbreekt of is ongeldig	digikoppeling compliant PKI-overheid certificaat.														
Client.EK0031	Berichtondertekening niet aanwezig of onjuist	Het bericht moet volgens contract ondertekend worden maar de ondertekening is ongeldig of niet aanwezig														
Server.EK0050*	Service afhandeling geeft fout	Het proces dat het serviceverzoek moet afhandelen geeft een fout														
43 B	DUO	<p>Aan foutcodes voorlooppullen toevoegen</p> <p>Voorstel</p> <p>in de lijst de voorlooppullen toe te voegen, bijvoorbeeld EK0020</p> <p>Besluit</p> <p>WG 14 januari 2021: Verwerken in 1.4</p>	Goedgekeurd	Midden	Laag	Laag	2									
46	DUO	<p>Ondersteunen van SNI</p> <p>Wij krijgen daarbij de vraag van onze ketenpartners met name in het VO</p>	Goedgekeurd	Midden	Midden	Midden	3									

	<p>en MBO om de SNI extensie ook te ondersteunen. SNI is een extensie op het TLS protocol.</p> <p>Het probleem waar onze ketenpartners, met name LAS-leveranciers van scholen, mee komen is het volgende: men heeft om voor hun moverende redenen op hun server nog andere webservices draaien met een niet-PKIO-certificaat. Dit frusteert het leggen van een TLS-tunnel waar een PKIO certificaat verplicht zoals bij ons. Als DUO een verkeerd certificaat aangeboden krijgt en komt geen TLS tot stand. DUO kan dit op eenvoudige wijze regelen door in de SNI-extensie de hostname op te nemen zodat de leverancier het juiste PKI certificaat voorschotelt.</p> <p>Voorstel</p> <p>In februari 2019 hebben we in de WG over SNI gesproken. Er is toen duidelijk geworden dat de OSO keten al enige tijd SNI toepast en ook Vroegtijdig Aanmelden MBO gaat dit voorschrijven. Navraag bij achterban van leden van de Edukoppeling werkgroep leverde wel op dat binnen het project Vroegtijdig aanmelden MBO geconstateerd was dat één partij met een SAP platform problemen had met SNI. Na een patch was dit opgelost. Met Oracle (Peoplesoft) is er waarschijnlijk nog wel een probleem en raakt 4 MBO instellingen.</p> <p>Verder heeft Logius de vraag bij verschillende leveranciers van Digikoppeling uitgezet of zij SNI ondersteunen. De vragen die aan de leveranciers gesteld zijn:</p> <ul style="list-style-type: none"> • Wat is de impact van het verplichten van SNI binnen de Digikoppeling standaard voor uw Digikoppeling implementatie/adapter? • Ondersteunt uw product zelf de optie SNI (d.w.z. meegeven hostnaam middels SNI)? of zijn hiervoor aanpassingen nodig?; • Als uw product de optie niet ondersteunt, is er dan ondersteuning in het platform waar uw product gebruik van maakt? (Voor zover u dit kunt overzien); • Welke impact zou het verplichten van SNI voor uw product hebben: Geen, beperkte of hoge impact?; <p>Bij het TO DK van 16 mei is hierover het volgende teruggekoppeld</p> <p>Er zijn 6 partijen die terugkoppeling hebben gegeven. Zij verwachten</p>	werkgroep UBV.				
--	---	----------------	--	--	--	--

		<p>hierbij de volgende impact:</p> <ul style="list-style-type: none"> • Drie leveranciers bieden ondersteuning en voorzien beperkte impact. • Drie leveranciers bieden geen ondersteuning: • Twee verwachten beperkte impact. • Eén leverancier verwacht hoge impact. <p>Bij het TO DK van 12 september is het SNI voorstel weer besproken. De TO DK leden geven aan niet direct behoefte te hebben aan SNI, maar kunnen zich wel voorstellen dat andere partijen in bepaalde scenario's behoefte aan kunnen hebben. Er wordt voorgesteld het als een best practice te documenteren.</p> <p>Nu het niet als voorschrift binnen DK gaat gelden moet er door werkgroep Edukoppeling besloten worden of we dit bij de uniforme beveiligingsvoorschriften onderwijs (UBO) gaan voorschrijven of binnen Edukoppeling. Omdat OSO hier al gebruik van maakt en SNI een configuratie is binnen TLS wordt voorgesteld dit bij UBO op te nemen (zie ook issue #22).</p> <p>Besluit</p> <p>WG 14 januari 2021: Niet relevant voor EK standaard, verplicht gebruikt SNI voor client is opgenomen in UBV Edukoppeling profiel.</p>					
47	Edustandaard	<p>Toestaan van pushberichten staat in architectuur, de afwijking op DK WB013 (actiepunt #89) moet in Best practice opgenomen worden</p> <p>Digikoppeling WUS versie 3.7 bevat een nieuw voorschrift (WB013) m.b.t ondertekenen en stelt: "Indien WS-Security wordt toegepast, is het controleren van de signature door de ontvangende partij verplicht".</p> <p>Volgens DK WB013 mag een antwoordbericht met invalide ondertekening niet verwerkt worden. Dit was eigenlijk al common practice. Het is alleen wel zo dat Edukoppeling ook push-berichten toestaat. Het niet verwerken van de response van een push-bericht vanwege een invalide ondertekening heeft geen effect. De service heeft feitelijk het push-bericht al verwerkt. De response was enkel een (technische) bevestiging.</p>	Goedgekeurd Verwerkt in BP 1.0	Midden	Midden	Midden	3

		<p>We hebben nu voor dit scenario een best practice gedefinieerd</p> <p>Voorstel</p> <p>Met het toestaan van push berichten in Edukoppeling wijken we af op Digikoppeling en hierdoor is andere formulering van WB013 noodzakelijk. Het toestaan van push-berichten staat in architectuur gedocumenteerd. We moeten de uitzondering op WB013 in een best practice documenteren.</p> <p>Ondertussen gaat DK wel pushberichten toestaan voor WUS en Logius is geïnformeerd dat we bij push bericht in BP een iets andere invulling geven(zie ook actiepunt #89).</p> <p>Besluit</p> <p>WG 18 maart 2020: Verwerkt in Best Practice</p>					