Concept Verslag ES werkgroep Edukoppeling transactiestandaard

Aanwezig: Edwin Verwoerd (Iddink, VDOD) , Gerald Groot Roessink (DUO), Marc Fleischeuers (Kennisnet, BPV/Vroegtijdig aanmelden MBO), Brian Dommisse (Kennisnet, voorzitter), Erwin Reinhoud (Kennisnet/Bureau Edustandaard).

Afwezig: Robert Kars (DUO), Peter Dam (Cito)

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

Datum en locatie
1 mei 2019, 10:00-13.00 uur, Seats2Meet, Amersfoort

Agenda

1. Opening, mededelingen, vaststellen agenda
2. Doornemen verslag en actielijst
3. Doorontwikkeling Edukoppeling
    a) Beheermodel versie 1.1
    b) Voorstel om ook voor Edukoppeling geen gelaagd versiebeheermodel toe te passen
    c) Opname SNI
    d) Gap met Digikoppeling
    e) Best Practices 0.9
    f) NCSC richtlijnen / Digikoppeling beveiligingsvoorschriften
4. Voortgang Edukoppeling – REST-profiel
5. Open punten issuelijst (nieuwe versie ondersteunende documenten)
6. Rondvraag / Sluiting

1. Opening, mededelingen, vaststellen agenda

De agenda wordt zonder wijzigingen vastgesteld.

Er wordt leden gevraagd om naar de achterban het bestaan van het discussieplatform te communiceren. Er zijn ondertussen 20 deelnemers.

1.1. Terugkoppeling Standaardisatieraad

Er wordt over de volgende onderwerpen terugkoppeling geven:

1. Centraal beheer voor beveiligingsvoorschriften voor S2S koppelingen
2. Edustandaard governance
3. Wettelijke verplichting rond beveiligingsstandaarden en toegankelijkheidsstandaarden

Centraal beheer voor beveiligingsvoorschriften voor S2S koppelingen
Vanuit de Edukoppeling werkgroep en de Architectuurraad is het advies gegeven om binnen het onderwijs beveiligingsvoorschriften (o.a. TLS) voor S2S koppelingen centraal te gaan beheren. Dit om te voorkomen dat bijvoorbeeld in OSO andere keuzes worden gemaakt dan bij Edukoppeling (Digikoppeling) en dit tot

interoperabiliteitsproblemen leidt. Het advies was om het beheer bij de Edustandaard IBP werkgroep te beleggen. Het beleggen van het beheer bij een (sub) werkgroep IBP leek niet goed te vallen bij de SR en er werd voorgesteld om dit toch bij Edukoppeling te beleggen. Wat het formele besluit vervolgens is geworden, is op dit moment nog niet duidelijk.
Vanuit de werkgroep wordt aangegeven dat partijen de beveiligingsvoorschriften niet altijd specifiek voor m2m-koppelingen moeten inrichten bijvoorbeeld omdat zij ook de beveiliging van de websites op hetzelfde platform hebben ingericht. Door het beleggen van de beveiligingsvoorschriften bij Edukoppeling ontstaat het beeld dat deze alleen voor m2m gelden terwijl het dus ook om websites gaat. De Edukoppeling werkgroep besluit dat het beleggen van de beveiligingsvoorschriften bij de IBP (sub) werkgroep de voorkeur heeft. Zij moeten ook duidelijk maken wat eventueel wel of niet voor m2m-koppelvlaken en/of websites geldt. Vanuit de Edukoppeling werkgroep is er al eerder met leden van de IBP werkgroep over dit onderwerp gesproken en beide werkgroepen hebben dezelfde beelden hoe dit vraagstuk opgelost moet worden. Er wordt besloten dat leden van de Edukoppeling werkgroep, IBP werkgroep en AR een advies opstellen voor de SR om het belang aan te geven (actiepunt #88).

Edustandaard is aan het onderzoeken hoe de governance van de afspraken beter ingericht kan worden.
Men wil hierbij ook met name het werken onder architectuur een plaats geven. Dit gaat mogelijk impact hebben op de verschillende werkgroepen. Er zijn werkgroepen specifiek voor een bepaald domein (zoals UWLR, ECK DT en Toetsen en examineren) en domeinoverstijgende werkgroepen (zoals IAA en Edukoppeling). Hierbij wil men tevens borgen dat besluiten van raden meer sturend worden (vergelijkbaar met een pas-toe-leg-uit regime). Een nieuwe governancestructuur moet dit mogelijk maken.

Wettelijke verplichting rond beveiligingsstandaarden en toegankelijkheidsstandaarden
Voor beveiligingsstandaarden en toegankelijkheidsstandaarden krijgt de minister van BZK in de wet Digitale Overheid de bevoegdheid deze als verplicht aan te wijzen in een AMvB. De juridische afdeling van OCW (WJZ) concludeert dat bekostigde scholen en onderwijsinstellingen binnen scope van deze wet vallen. Er is ruimte gecreëerd (art.3.3e lid) om een nadere scope bij AMvB te bepalen, maar dat kan alleen als er een heel sterk verhaal onder ligt (proportionaliteit). En een AMvB kan niet afwijken van de bovenliggende EU richtlijn. Deze geeft aan dat dat content die verband met houdt met wezenlijke online administratieve functies van scholen (denk hierbij aan inschrijven) niet uitgezonderd mag worden (zie voor meer details https://www.edustandaard.nl/app/uploads/2019/03/Bijlage-4.-Notitie-opnemen-wettelijk-voorgeschreven-standaarden-in-de-ROSA.pdf). In de SR is besproken of deze (wettelijk verplichte) rijksbrede standaarden in de ROSA opgenomen kunnen worden en welke procesafspraken nodig zijn om impact te bepalen per toepassingsdomein.

De verwachting vanuit de werkgroep is dat het met name sites zal betreffen waarbij een (administratieve) dienst wordt aangeboden aan een burger, zoals de aanmelding via Studielink. Daarnaast is het onderwijs al ingericht om voor bepaalde doelgroepen toegankelijkheid goed te ondersteunen (bijvoorbeeld Speciaal Onderwijs en het Voortgezet Speciaal Onderwijs). Er wordt geconcludeerd dat deze beveiligingsstandaarden en toegankelijkheidsstandaarden goed aansluiten bij wat eerder is besproken rond beveiligingsvoorschriften voor m2m-koppelingen die waarschijnlijk bij de IBP werkgroep belegd gaan worden.

1.2. Ervaringen bij het gebruik van de Digikoppeling compliancevoorziening

De Digikoppeling compliancevoorziening is door Kennisnet getest met een Edukoppeling implementatie. De compliancevoorziening levert geen rapport met alle bevindingen, maar er wordt per test 1 bevinding gemeld. Dit maakt de compliancetest wat omslachtig en afhankelijk van de fout wordt ook pas duidelijk wat er mis is na communicatie met de applicatiebeheerder. Wat we tot nu toe weten:

1. Een Edukoppeling 2W-be profiel wordt ondersteund en kan getest worden. Het 2W-be-S (en wellicht 2W-be-SE) kan nu niet getest worden: In Digikoppeling zijn de WSA ReplyTo en WSA From header in het request optioneel. De compliancevoorziening vereist bij het 2W-be-S (niet bij het 2W-be profiel) een WSA ReplyTo in het request en deze moet bij het 2W-be-S profiel ook ondertekend zijn. Het WSA From veld lijkt juist niet voor te mogen komen in het request.
2. De compliancevoorziening geeft een ‘No Subject DN Certificate Constraints were defined’ warning. Waarschijnlijk ontstaat deze warning als er geen direct trust is (publiek certificaat zit niet in truststore

maar wordt meegeleverd met het bericht). Bij het 2W-be-S profiel is het common practice dat het publieke deel van het certificaat met bericht uitgewisseld worden. Er lijken verschillende beveiligingsniveaus te zijn die in de standaard niet onderkend worden.

De ervaringen zijn met Logius gedeeld en voor het eerste punt is een issue geregistreerd. Logius zal melden als het issue is opgelost. We besluiten om op het community platform een melding op te nemen dat tot nader order de Digikoppeling compliancevoorziening niet gebruikt kan worden voor het 2W-be-S(E) profiel.

1.3. Rapport Verkenning API's van Logius

Logius heeft laten onderzoeken wat de ontwikkelingen rond REST/API's voor Logius betekent (Verkenning API's[1]). De vraagstukken en adviezen in dit document zijn ook relevant voor de positionering van REST binnen Edukoppeling. Indien mogelijk is het wenselijk om de lijn van Logius te volgen.

Het rapport stelt dat het overkoepelende toepassings- en werkingsgebied voor Digikoppeling ongewijzigd blijft. Het toepassingsgebied van RESTful gegevensuitwisseling overlapt gedeeltelijk met Digikoppeling. Er wordt geadviseerd om de interactiepatroon nader uit te werken. Voor bevragingen vanuit apps en gebruikerstoepassingen van burgers en bedrijven is het gewenst toe te werken naar voorschrijven van REST API's. Dit zal op den duur bepaalde van de huidige WUS bevragingen vervangen. Qua verwachtingen en communicatie is het belangrijk te benadrukken dat dit enerzijds een volwaardige variant is, maar anderzijds de behoefte aan de bestaande varianten WUS en ebMS niet wegneemt. Er is geen reden bestaande koppelingen uit te faseren of om te bouwen. Voor transacties en meldingen die reliable messaging vereisen (ebMS) vormt REST, zeker voorlopig, geen alternatief.

Verder wordt gesteld dat de nieuwe technologische mogelijkheden tot verschuiving van de architectuur kunnen leiden: van uitgebreide webapplicaties – veelal met nog restanten van vroegere papieren formulieren – met daarachter ketenprocessen naar apps voor een specifieke taak – meer levensgebeurtenis georiënteerd. Deze volgende stap in de digitalisering kan gepaard gaan met procesvereenvoudiging. Als de technologische mogelijkheden goed benut worden, kan dit leiden tot minder complexe ketenprocessen en dus uiteindelijk tot afname van de behoefte aan de huidige berichtuitwisselingsstandaarden.

Een aantal aanbevelingen uit het rapport zijn opgenomen in bijlage A.

2. Doornemen verslag en actielijst van 13 februari 2018

Het verslag van 13 februari wordt zonder wijzigingen vastgesteld.

Actiepunt #77 Documenteren van push en pull variant
Afgehandeld, verwerkt in best practice 0.9. Het architectuurdocument beschrijft dit interactiepatroon al. In de BP wordt hier iets dieper op ingegaan.

Actiepunt #80 Code van DUO of het WUS Signing onderzoek van Logius beschikbaar stellen
De code van DUO wordt nog beschikbaar gesteld.
Actiepunt blijft nog open.

Actiepunt #82 Navraag doen bij Logius of het gebruik van SNI opgenomen kan worden
Afgehandeld. Wordt nog wel besproken bij agendapunt 3 – Opname SNI

Actiepunt #85 Onderzoek of (bepaalde versies) SAP en Oracle SNI ondersteunen
Afgehandeld. Wordt nog wel besproken bij agendapunt 3 – Opname SNI

[1] https://docs.google.com/viewer?a=v&pid=forums&srcid=MDAwNDA0Njg2MjczMDg3MTM1MjMBMTQ4Mzc3NDI3MjMwMTM4NTQxMDIBaGZCU214YXJCUUFKATAuMgFrZW5uaXNuZXQubmwBdjI&authuser=0

Actiepunt #86 Onderzoeken of een foutieve ondertekening van response afgekeurd moet worden en niet verwerkt mag worden

Afgehandeld. Verwerkt in BP 0.9. Wordt nog bij agendapunt 3 besproken i.v.m. Digikoppeling WB013

Actiepunt #87 Agenderen overkoepelende versie of samenstelling met versie op documentniveau (conform Digikoppeling).

Afgehandeld**.** Zie agendapunt 3 - Voorstel om ook voor Edukoppeling geen gelaagd versiebeheermodel meer toe te passen, maar de nieuwe methodiek van Digikoppeling te volgen.

3. Doorontwikkeling Edukoppeling

3.1. Beheermodel versie 1.1

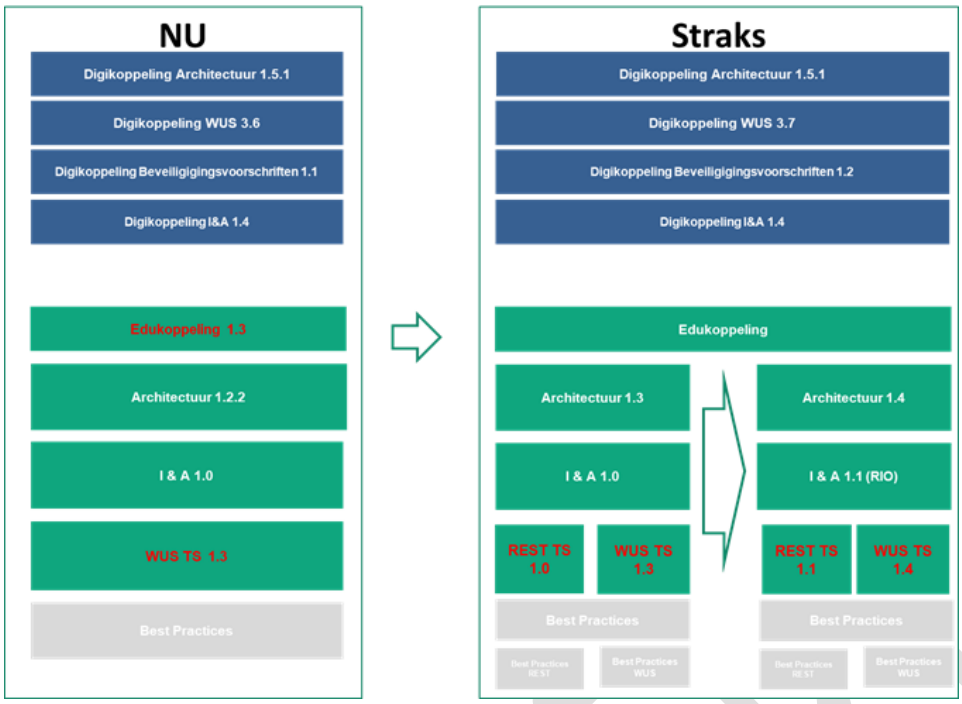
Digikoppeling gebruikt de versioneringsmethodiek Major, Minor en Patch. Het Edukoppeling Beheermodel is hierop aangepast en is ook iets anders gestructureerd.

- Patch release
  In een patchrelease worden wijzigingen doorgevoerd die de technische specificatie niet raken. Dit zijn over het algemeen categorie 1&2 issues. Dit kunnen tekstuele wijzigen zijn of inhoudelijke indelingen van de documenten. De wijzigen worden vastgelegd in release notes. Een patch release wordt door de beheerder op eigen initiatief of op aanwijzingen van gebruikers doorgevoerd en gepubliceerd. Een patchrelease wordt aan de Architectuurraad ter kennisgeving medegedeeld. Een nieuwe patchrelease vervangt net als de andere niveaus een eerdere versie in zijn geheel.
- Minor release
  In een minor release kunnen wijzigingen doorgevoerd worden die de technische specificatie van een koppelvlak raken. Dit zijn over het algemeen categorie 3 issues met een gemiddelde impact. In de SEMVER aanpak zijn minor releases backwards compatible. Hiermee zouden minor release vaak beperkt worden tot alleen verruimende wijzigingen. Zo zou een toevoeging van TLS 1.3 in een Minor release kunnen, maar het uitfaseren van TLS 1.2 zou een Major release zijn. Voor de Digikoppeling standaard lijkt backwards compatibility lastiger te bepalen en heeft men er voor gekozen dat Minor Releases mogelijk backwards incompatible kunnen zijn. Voor Minor Releases wordt daarom altijd een uitgebreid vaststellingsprocedure gevolgd (conform het Digikoppeling Beheermodel) en er kan in overleg met de deelnemers van het TO tot een migratiepad worden besloten. Dit migratiepad wordt in de release meegenomen. Voor Edukoppeling wordt voor Minor Releases ook een vaststellingsprocedure gevolgd naar de Architectuur- en Standaardisatieraad.
- Major release
  Er zijn twee Major release momenten: de overgang naar nieuwe internationale standaarden binnen een bestaand profiel, bijvoorbeeld HTTP 2.0 of SOAP 1.2 binnen WUS of de toevoeging van een geheel nieuw profiel. Dit zijn over het algemeen categorie 4 issues met een hoge impact. Voor een nieuwe Major Release wordt de uitgebreide vaststellingsprocedure gevolgd.

Voor verdere details wordt verwezen naar de 1.1 versie van het beheermodel (paragraaf 5.7).

3.2. Voorstel om ook voor Edukoppeling GEEN gelaagd versiebeheermodel toe te passen

Digikoppeling had een gelaagd versiebeheermodel (op het niveau van de set en de individuele documenten), maar heeft nu versionering op het niveau van beschrijvende documenten. Er wordt voorgesteld om Digikoppeling ook op dit punt te volgen en niet meer de overkoepelende Edukoppeling versie te hanteren. Deze overkoepelende versie is momenteel aan de Transactiestandaard gekoppeld (versie 1.3). Ook gezien de komst van een REST Transactiestandaard is dit minder wenselijk. Bij een implementatie zou men alsnog moeten communiceren welke versie van de Transactiestandaard geïmplementeerd wordt.



Er wordt besloten om het voorstel over te nemen en de versie aan te duiden op basis van de versie van de documenten (besluit #14).

Voor een bepaalde implementatie is met name de versie van de transactiestandaard (REST / WUS) relevant. Hoe deze samenhangt met de versie van de andere normatieve documenten van de standaard (Architectuur of I&A) moet wel extra aandacht krijgen. Er wordt voorgesteld om conform Digikoppeling een Compliance en overzicht document op te stellen met hierin een tabel met de verschillende versies en hun status. Als voor een bepaald document een nieuwe versie komt dan wordt aangegeven tot welke datum de oude versie de status 'in gebruik' behoudt. Na deze datum krijgt het document de status 'Einde ondersteuning'. Er worden dan voor die versie geen wijzigingen meer geaccepteerd. De werkgroep heeft de verantwoordelijkheid om er op toe te zien dat een logische samenhang tussen de vigerende versies gewaarborgd is.

Voor ketens die een bepaald REST of WUS profiel implementeren is het wel raadzaam om in het programma van eisen niet alleen de versie van de transactiestandaard op te nemen maar ook de versie van de andere normatieve documenten (inclusief de relevante Digikoppeling documenten). Hoewel het geadviseerd wordt om in een keten de vigerende versie van Edukoppeling te volgen, kan met opname van de versies in het programma van eisen inzichtelijk blijven welke versies geïmplementeerd zijn binnen de keten.

Publicatie op Edustandaard

Een ander aandachtspunt is communicatie. We willen een duidelijk overzicht hebben van de verschillende versies op de Edustandaard site. Deze informatie wordt al opgenomen in het nog op te stellen compliance- en overzichtdocument, maar het is goed als deze informatie ook op de site inzichtelijk wordt gemaakt. Hierbij kan tevens de relatie met Digikoppeling expliciet aangeven worden.

3.3. Opname SNI

Eerder is vanuit DUO aangegeven dat er behoefte is aan ondersteuning van SNI. SNI is nodig omdat partijen meerdere certificaten bij services gebruiken. Zonder SNI kunnen deze partijen mogelijk niet koppelen omdat de server mogelijk het verkeerde PKI certificaat aanbiedt.

De huidige status is het volgende:

- Er is reeds een issue voor SNI geregistreerd (#46).
- Het SAP platform had een probleem, maar is met een patch opgelost.
- Het Oracle (Peoplesoft) platform heeft nog steeds een probleem met ondersteuning hiervan.

- Binnen het onderwijs willen we de voorschriften rond TLS en ciphers centraal gaan beheren en waarschijnlijk hoort ook SNI hierbij.
- Logius heeft bij verschillende leveranciers van Digikoppeling de vraag uitgezet of zij SNI ondersteunen. Hierover wordt bij het volgend TO DK terugkoppeling over gegeven (16 mei 2019). Het is nu nog niet zeker of DK optioneel gaat toestaan.

Gezien de zaken die nog open staan wordt er besloten deze ontwikkelingen af te wachten. Wel is het dus zo dat enkele partijen met het Oracle platform hier dus niet aan kunnen voldoen. Deze situatie zien we bij SNI maar zullen we ook in de toekomst tegen blijven komen. Bijvoorbeeld bij de ondersteuning van TLS versies en ciphers. Niet alle partijen zullen direct de wijzigingen kunnen doorvoeren. Verder moeten we een balans vinden met de standaard waarbij we aan beveiligingsvoorschriften voldoen, maar partijen niet (direct) uitsluiten. Zij moeten de tijd krijgen om te migreren. Het is dus belangrijk om met migratiefases te werken en deze tijdig te communiceren. In praktijk blijkt het echter lastig om partijen te bereiken. We weten dat de OSO keten hier al mee werkt en de ondersteuning voor SNI is ook in het Programma van Eisen voor Vroegtijdig Aanmelden opgenomen. Dit helpt in de communicatie en zorgt ervoor dat partijen hun platformen hierop inrichten. Een IBP (sub) werkgroep kan helpen bij het vaststellen van een passende migratiefase.

In de periode naar de volgende release van Edukoppeling moet duidelijk zijn of SNI onderdeel is van Digikoppeling en/of een IBP werkgroep het beheer voert over onderwijsbrede beveiligingsvoorschriften. Als SNI niet in Digikoppeling wordt opgenomen en niet centraal bij IBP belegd wordt, dan zal er binnen Edukoppeling een voorstel opgesteld worden en ter consultatie worden aangeboden als onderdeel van een volgende release.

3.4. Gap met Digikoppeling

Ook de Digikoppeling standaarden worden doorontwikkeld. Zo zien we dat o.a. de beveiligingsvoorschriften worden aangepast en dat na het onderzoek rond ondertekenen ook de koppelvlakstandaard WUS op een paar punten wordt aangepast. De doorontwikkeling van Digikoppeling zorgt in principe voor een gap met Edukoppeling. Er is echter afgesproken dat Edukoppeling meebeweegt met Digikoppeling zonder hiervoor een nieuwe versie te publiceren. Het is wel de verantwoordelijkheid van de werkgroep om deze gaps te onderkennen en de impact ervan te bepalen. Sommige wijzigen zullen geen impact hebben, maar anderen zullen vereisen dat er actief hierover naar de Edukoppeling community gecommuniceerd wordt. Dit is bijvoorbeeld het geval bij aanpassingen van de TLS versies en ciphers (zolang het beheer van TLS niet bij IBP is belegd). Bij Digikoppeling zien we de volgende wijzigingen:

- Er is een conceptversie van de koppelvlakstandaard WUS (versie 3.7). Hierin zitten o.a. de volgende wijzigingen:
  - De WSA:To header in de response is optioneel geworden
    - We hebben hierop al geanticipeerd in de Edukoppeling TS versie 1.3 (WSA:To is en blijft verplicht).
  - Een nieuw voorschrift WB013 m.b.t ondertekenen dat stelt: “Indien WS-Security wordt toegepast, is het controleren van de signature door de ontvangende partij verplicht”. 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. We hebben nu voor dit scenario een best practice gedefinieerd (zie bijlage B). We wijken hiermee dus af op Digikoppeling WB013. Er wordt besloten om het toestaan van push-berichten en de afwijking op WB013 op te nemen in de volgende release van de Transactiestandaard (actiepunt #89)
- Er is een conceptversie van de Digikoppeling Beveiligingsstandaarden en voorschriften (versie 1.2). Hierin zijn de adviezen van de NCSC Handreiking TLS (v2.0) verwerkt. De wijzigingen hierin worden later in detail toegelicht bij de bespreking van de NCSC handreiking. Er wordt dan tevens besproken wat er aan Logius over de Beveiligingsstandaarden versie 1.2 teruggekoppeld wordt. Er wordt wel al besproken dat de wijzigingen met name impact hebben op de ciphers die bij TLS toegepast mogen worden. Ook op dit punt is het wenselijk om met Digikoppeling mee te bewegen (net als dat op termijn ook geldt als deze voorschriften wellicht vanuit IBP opgesteld worden), maar gezien de impact moet hierover wel gecommuniceerd worden en zal een passende migratiefase noodzakelijk zijn. Er wordt voorgesteld om e.e.a. op community platform te communiceren en op te nemen in Edustandaard nieuwsbrief (actiepunt #90).
- Mogelijk zal aan de conceptversie ook SNI toegevoegd worden.

3.5. Best practices 0.9

Er is een nieuwe versie van de best practices. De volgende issues zijn in de 0.9 versie verwerkt:

- Issue 9 – Versioning : Bij Paragraaf 2.3 ‘Tijdig vaststellen welke versie toegepast moet worden’ eea over versioning opgenomen. Dit kan nog aangevuld worden op basis van ervaringen in ketens.
- Issue 30 - Vulling WSA Action bij SoapFault
- Issue 31 - Request zonder WSA From of zonder OIN (fout 20 of 21)
- Issue 32 - Request bevat header dat geen onderdeel is van een Edukoppeling profiel. Wat moet er dan worden teruggestuurd.
- Issue 34 - Validatie certificaat tegen Certificate Revocation List PKI Overheid
- Issue 35 - Validatie hiërarchie van certificaat. Hoe gaat de validatie van de hiërarchie van het certificaat in zijn werk?

We willen nog een aantal zaken in de best practice verwerken waarna een 1.0 versie gepubliceerd zal worden. We verwachten wel dat met de komst van een REST profiel e.e.a. gewijzigd zal moeten worden. We denken aan een generiek deel en specifiek best practice document per transactiestandaard.

3.6. NCSC richtlijnen TLS (versie 2.0) en Digikoppeling Beveiligingsvoorschriften (versie 1.2)

NCSC richtlijnen TLS (versie 2.0)

Een aantal aspecten uit de richtlijnen voor TLS van het NCSC worden toegelicht.

- Er zijn nu 4 beveiligingsniveaus voor certificaatverificatie, sleuteluitwisseling, bulkversleuteling en hashing opgenomen. Er is een niveau Onvoldoende, Uit te faseren, Voldoende en Goed
    - Het beveiligingsniveau 'uit te faseren' is nieuw en geeft aan dat binnen een bepaald vastgesteld termijn (te bepalen door keten/sector zelf) bepaalde instellingen niet meer gebruikt mogen worden. Voorbeelden van uit te faseren instellingen zijn: TLS 1.0, TLS 1.1, 3DES en statische sleuteluitwisseling (TLS_RSA_...)
- Gebruik liever ECDHE dan DHE.
    - Wordt DHE gebruikt? Dan gelden eisen voor de gebruikte parameters.
- Er is expliciet iets over beheer opgenomen en we verachten dat men meer proactief beheer gaat voeren. Dit betekend ook dat we binnen het onderwijs hiermee om moeten kunnen gaan. Het centraal beleggen van beveiligingsvoorschriften bij IBP gaat hierbij helpen. Zij zullen echter wel korte lijnen naar implementaties moeten hebben.
    - NCSC over het beheer van de richtlijnen: ‘*Indien er een acute wijziging van deze richtlijnen nodig is, dan zal deze worden uitgebracht als addendum bij de meest recente versie van de richtlijnen. Een dergelijke situatie kan zich bijvoorbeeld voordoen als uit onderzoek blijkt dat bepaalde TLS-configuraties niet meer veilig zijn*
- Er wordt geadviseerd om TLS 1.0 en TLS 1.1 uit te faseren. Binnen het onderwijs wordt over het algemeen al TLS 1.2 gebruikt indien van toepassing (uitwisseling persoonsgegevens).
- De TLS 1.3 versie is toegevoegd.
- Andere codering voort ciphers bij TLS 1.3. Tot en met TLS 1.2 bestond een cipher suite ook uit de algoritmes voor sleuteluitwisseling en digitale handtekeningen. Dit resulterende in een enorm aantal combinatiemogelijkheden voor cipher suites. De cipher suites in TLS 1.3 bestaan alleen nog maar uit de algoritmes voor bulkversleuteling en hashing.

Digikoppeling Beveiligingsvoorschriften 1.2

Een aantal wijzigingen in de Digikoppeling beveiligingsvoorschriften worden toegelicht.

- TLS003:
  - Oud: ”*De TLS implementatie mag niet op SSL v3,SSL v2, SSL v1 terug kunnen vallen*”
  - Nieuw: ”*De TLS implementatie mag niet op SSL v3 terug kunnen vallen*”
- TLS004:
  - Oud:*” TLS 1.0 en TLS 1.1 zijn niet meer toegestaan Niet meer toegestaan vanaf 10-9-2016”*
  - Nieuw: “*Het is verplicht TLS 1.2 of TLS 1.3 te gebruiken*”
- TLS006 (nieuw): “*Het is verplicht te voldoen aan de NCSC ICT-beveiligingsrichtlijnen voor TLS*“
- TLSCIPH001:
  - Oud:“*De onderstaande TLS encryptie algoritmen en sleutellengtes MOETEN minimaal worden ondersteund:*
    - *TLS_RSA_WITH_AES_256_CBC_SHA*
    - *TLS_RSA_WITH_AES_128_CBC_SHA*“
  - Nieuw: “*Voor TLS 1.2*: *De gebruikte TLS cryptografische algoritmen moeten de NCSC classificatie ‘voldoende’ of ‘goed’ hebben. Het onderstaande TLS cryptografische algoritme MOET minimaal worden ondersteund:*
    - *TLS_ECDHE_RSA_WITH_AES_128_GCM_ SHA256*[2]

    Voor TLS 1.3: Het onderstaande TLS cryptografische algoritme MOET minimaal worden ondersteund:
    - *Sleutel uitwisseling: ECDHE*
    - *Certificaat verificatie: RSA*
    - *Bulk encryptie: AES_128_GCM*
    - *Hashing: SHA256*[3]*”*
- TLSCIPH002: Sterk aanbevolen ciphers voor TLS 1.2 zijn vervallen en de cipher suites met kwalificatie “goed” en ”voldoende” voor TLS 1.2 zijn gewijzigd. Voor TLS 1.3 zijn cipher suites met kwalificatie “goed” en ”voldoende” toegevoegd
- ENC003 (origineel is vervallen): De ondersteunde data encryption (data versleuteling) algoritmen zijn: 3DES, AES128, AES256. Gebruik GCM mode indien beschikbaar anders CBC mode in combinatie met een signature [AES128-CBC], [AES128-GCM], [AES256-CBC], [AES256-GCM]
- ENC004: Het Key transport algorithm maakt gebruik van de RSA-OAEP algoritmen (RSA1_5 verwijderd)
- ENC005: Vervallen (Dit is voorschrift ENC004 geworden)

Punten die tot nu toe teruggekoppeld worden aan Logius:

1. Na bijna 5 jaar is er een update van de NCSC TLS handreiking. In de NCSC handreiking hebben we bij het onderdeel ‘Wijziging van deze richtlijnen’ gezien dat er (nu) actief beheer wordt gevoerd. We verwachten dat er met een addendum sneller geacteerd wordt op gewenste updates. Het is wenselijk om (voorlopig) periodiek ontwikkelingen te blijven volgen binnen het TO DK. We kunnen dan als TO DK besluiten of de keuzes rond TLS en ciphers actueel blijven.
   a) Toelichting: Binnen het onderwijs hebben we een jaar lang een interoperabiliteitsprobleem gehad omdat Digikoppeling en hiermee ook Edukoppeling nog de handreiking uit 2014 volgden. Binnen onderwijsketens waren de voorschriften al eerder aangescherpt (TLS_RSA_... ciphers werden al niet meer toegestaan) op basis van andere referenties dan NCSC (o.a. Mozilla en Qualys). We streven naar het gebruik van NCSC als referentie, maar daarbij geldt wel als voorwaarde dat de beveiligingsmaatregelen hiervan actueel zijn. Het onderwijs zal zelf actief ontwikkelingen rond beveiliging (TLS) blijven volgen en onafhankelijk actie nemen indien noodzakelijk.
2. Het voorstel om alleen ‘goede’ GCM suites minimaal verplicht te stellen voor Digikoppeling is in principe wenselijk. We adviseren om voor CBC suites wel een passende migratieperiode te hanteren en dat

[2] Bij het Edukoppeling overleg is een eerdere conceptversie van de Beveiligingsvoorschriften versie 1.2 besproken. Hierin waren voor TLS 1.2 nog TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA en TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA als minimale ciphers opgenomen. Dit is nu dus TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 geworden. Vanuit Kennisnet/Edukoppeling is op deze wijziging teruggekoppeld dat hiervoor een migratiefase voor onderkend moet worden. We verwachten dat deze 2 jaar moet zijn, maar moet door TO Digikoppeling vastgesteld worden

[3] Zie terugkoppeling aan Logius Hashing: SHA256 moet waarschijnlijk SHA384 zijn

gedurende deze periode de CBC suites de status ‘uit te faseren’ krijgen en nog wel toegepast kunnen worden. We verwachten dat de migratieperiode enkele jaren zal moeten zijn, maar moet worden vastgesteld door de Digikoppeling community.

3. Voor referenties naar cipher suites wordt in de NCSC handreiking de IANA codering gebruikt. In Digikoppeling wordt deze codering overgenomen. Er is echter ook een OpenSSL en Hex codering. Wellicht is het goed om een referentietabel op te nemen in het document.
4. TLSCIPH001: Voor TLS 1.2 worden twee ciphers genoemd waar minimaal aan voldaan moet worden, voor TLS1.3 maar 1. Benoem voor TLS 1.2 alleen TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA waar minimaal aan voldaan moet worden.
5. TLSCIPH002: Sterk aanbevolen: voor TLS 1.3 wordt voor hashing SHA256 genoemd, maar hier wordt waarschijnlijk SHA384 bedoeld.
6. Het betreft versie 1.2, maar in voettekst van het document staat nog 1.1

Na afstemming met de Security Officer van Kennisnet zal dit naar Logius gestuurd worden en op het Edukoppeling Community Platform geplaatst worden.

4. Voortgang Edukoppeling – Transactiestandaard REST

De laatste versie van de Transactiestandaard REST is op het Community Platform geplaatst en zal ter consultatie aangeboden worden. In deze versie zijn een aantal kleine wijzigingen doorgevoerd.

Eerder is de vraag naar voren gekomen of canonicalization van de (JSON) content nodig is. Dit wordt inderdaad toegepast en er is hiervoor al een standaard beschikbaar (JCS[4]). De JCS specificatie is op weg om een dergelijk algoritme te standaardiseren. De simple canonicalization die nu in de Transactiestandaard opgenomen is zal voor een groot deel van de situaties gelijk zijn aan JCS. De JCS specificatie gaat verder dan de Edukoppeling Transactiestandaard REST in de manier waarop de basis datatypes worden weergegeven, met name bij de weergave van getallen (decimalen, machten) en strings met bijzondere unicode karakters. De verwachting is echter dat dergelijke waarden niet vaak voorkomen in JSON objecten. Als dat wel het geval gaat worden, moet de Edukoppeling Transactiestandaard REST verder worden aangevuld of moet er gemigreerd worden naar de (hopelijk tegen de tijd vastgestelde) RFC van JCS.

Er wordt aangegeven dat op nationaal niveau (Kennisplatform API’s) nu nog geen aandacht is voor het kunnen ondertekenen van RESTful berichten (payload). Op 24 mei zal de Edukoppeling Transactiestandaard REST aan het Kennisplatform API’s toegelicht worden.

Er is nog wat onduidelijkheid rond het nut van de Transactiestandaard REST. Er wordt aangegeven dat de Transactiestandaard WUS nu drie profielen heeft, een best effort profiel, een profiel voor het ondertekenen en een profiel voor ondertekenen en versleutelen. Het ondertekenen wordt gebruikt als onweerlegbaarheid en/of integriteit bij uitwisseling noodzakelijk is. Bij een RESTful uitwisseling willen we soms ook onweerlegbaarheid en/of integriteit ondersteunen. Er is hiervoor nu geen standaard beschikbaar. Wel zijn er standaarden die als basis gebruikt kunnen worden. Het Edukoppeling Transactiestandaard REST is een beperkte set voorschriften die op deze standaarden voortbouwt. Dit is vergelijkbaar met hoe Edukoppeling voortbouwt op Digikoppeling. Hoewel het bij het OSR om publieke informatie gaat wordt het REST profiel met ondertekenen hier toegepast om onweerlegbaarheid en integriteit te ondersteunen. Verder hadden de belanghebbenden een voorkeur voor een RESTful implementatie boven de Transactiestandaard WUS.

De werkgroep verwacht wel dat er vragen zullen zijn wanneer WUS of REST nu wel of niet toegepast moet/mag worden. Het is wenselijk om dit te documenteren. De Standaardisatieraad zal voor de onderwijssector moeten besluiten wat de verschillende werkings- en toepassingsgebieden zijn. Als eerste stap wordt hiervoor op het discussieplatform een post geplaatst om de discussie hierover te starten (actiepunt #91). Dit moet vervolgens ook in de Edukoppeling documentatie opgenomen worden.

[4] https://cyberphone.github.io/ietf-json-canon/

5. Issuelijst

Er was geen tijd meer over om de issuelijst door te nemen. Deze wordt voor het volgende overleg geagendeerd.

6. Rondvraag en sluiting

Geen punten meer voor de rondvraag. De volgende werkgroep zal na de zomer (september) worden gepland.

Actielijst

#	Omschrijving	Status	Einddatum	Actie-houder	Prio
77	Documenteren van push en pull variant in best practices	Loopt	Q2 2019	BES	2
80	Code van DUO of het WUS Siginging onderzoek van Logius beschikbaar stellen	Loopt	Q2 2019	BES /DUO	2
82	Navraag doen bij Logius of het gebruik van SNI opgenomen kan worden	Februari 2019	Q1 2019	DUO	2
85	Onderzoek of (bepaalde versies) SAP en Oracle SNI ondersteunen,	Nog inplannen	Q2 2019	BES	2
87	Agenderen overkoepelende versie of samenstelling met versie op documentniveau (conform Digikoppeling).	Afgerond	Q2 2019	BES	2
88	Advies voor SR opstellen: beveiligingsvoorschriften centraal beheerd door IBP	Nog inplannen	Q3 2019	IBP/Edukoppeling en AR	1
89	Met de Best practice rond WB013 wijken we af op Digikoppeling. Dit omdat Edukoppeling ook push-berichten toestaat. We willen dit in de volgende release van de Transactiestandaard opnemen	Nog inplannen	Q4 2019	BES	2
90	De wijzigingen rond Digikoppeling beveiligingsvoorschriften (TLS ciphers) communiceren op community platform en Edustandaard nieuwsbrief.	Nog inplannen	Q3 2019	BES	1
91	Op het discussieplatform een post plaatsen over het werkings- en toepassingsgebied van het REST en WUS profiel. Dit is de basis voor het voorstel aan de standaardisatieraad.	Nog inplannen	Q3 219	DUO (Gerald)	1

BES = Bureau Edustandaard
Grijs = afgehandeld of vervallen

Besluiten

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

7. Bijlage A: Verkenning API's - Adviezen aan Logius

In het rapport zijn o.a. de volgende adviezen opgenomen:

- Kies ervoor om REST API's als variant toe te voegen aan de Digikoppeling standaard. Het toevoegen biedt de beste mogelijkheden om aan te geven hoe de verschillende varianten zich tot elkaar verhouden en samenwerken en is de kortste route naar opname van API-gewijze dienstverlening als optie binnen de PTOLU standaarden.
- Omarm het "eating your own dog food" adagium. Neem dit voor een aantal voorzieningen op als eis voor verdere doorontwikkeling. MijnOverheid en DigiD liggen daarbij het meest voor de hand. Kies vanwege de samenhang tussen interne en externe koppelingen voor opname van een derde variant voor RESTful API's binnen de bestaande Digikoppeling standaard. Daarmee blijft de naam "Digikoppeling" als dè standaard voor gegevensuitwisseling tussen overheden in stand.
- De zogenoemde API-strategie van DSO biedt een goed uitgangspunt voor de benodigde afspraken voor een REST API variant binnen Digikoppeling. DSO heeft geen belang bij het beheer hiervan op langere termijn. Deze werkwijze wordt nu al in het kennisplatform API's gevolgd. De meest pragmatische werkwijze is om een en ander eerst losstaand te realiseren en in de bestaande Digikoppeling standaard te verwijzen naar deze ontwikkeling. Daarna is het gewenst o.a. het Digikoppeling architectuurdocument aan de nieuwe ontwikkelingen aan te passen zodat een samenhangend geheel ontstaat.
- Afronding van het Nederlandse Oauth profiel betekent dat de belangrijkste belemmering voor standaardisatie wordt weggenomen. Dit profiel wordt momenteel beschreven in kennisplatform. Dit biedt een goed momentum om de uitbreiding van Digikoppeling aan te kondigen.
- In vervolg op Oauth dient ook een profiel voor Open ID Connect te worden vastgesteld. Net als voor Oauth kan hiervoor aangesloten worden op een internationale profiel.
- Dit zou betekenen dat Logius tenminste een deel van de doelstellingen van het kennisplatform API's tot haar taak gaat rekenen. Dit dient uiteraard in goed overleg en vanuit een faciliterende inzet naar de belangen van het hele ecosysteem te worden ingericht.
- Veranker de uitgangspunten van Common Ground[5] expliciet in de architectuur en werk vanuit draagvlak en gezamenlijkheid aan een standaardisatie die ook op de ontwikkelingen bij gemeenten en andere bestuurslagen aansluit. Maak daarbij tijdig afspraken over de overgang van de huidige op innovatie gerichte ontwikkeling van o.a. NLX en het belang tijdig voor te sorteren op een stabiele beheer, opschaal en doorontwikkelfase. Dat laatste is een mogelijke rol voor Logius.
- Doe nader onderzoek naar effect van API-gewijze interactie op semantische standaarden. Indien dit het vermoeden bevestigt dat de semantische operabiliteit goed kan worden behouden, kan een overgangsregeling worden opgesteld in de vorm van een best practice. Daarmee zouden formele belemmeringen voor API-gewijze dienstverlening in betreffende toepassingsgebieden worden voorkomen. Dit onderzoek is eerder een taak van Forum Standaardisatie dan van andere Logius onderdelen.
- Uit enkele van de interviews zijn relevante juridische vragen naar boven gekomen. In het bijzonder de vraag in hoeverre API-gewijze dienstverlening op gespannen voet staat met doelbinding. De wendbare inrichting van API-gewijze dienstverlening kan er toe leiden dat het doel van de gebruiker onzichtbaar is voor de betrokkenen. Het doorgeven van een "doelbindingsverklaring (declaration of purpose)"[6] als voorgesteld door Common Ground biedt een goede oplossing voor het behoud van doelbinding in een zeer wendbaar APIecosysteem. Vraag aan het ministerie van BZK om in kaart te brengen wat er al over dit vraagstuk uitgewerkt is. Vermoedelijk zijn deze vraagstukken op basis van goede doordenking van de AVG oplosbaar.

[5] https://github.com/VNG-Realisatie/common-ground/blob/master/cg-vision.md

[6] https://github.com/VNG-Realisatie/common-ground/blob/master/cg-vision.md#moving-from-manual-toautomated-accountability

8. Bijlage B: Best Practice (versie 0.91) Invalide ondertekening van een push-bericht response

Digikoppeling WUS wordt alleen voor bevragingen (pull) gebruikt en ondersteund in principe geen meldingen (push). Voor Edukoppeling geldt de volgende aanvulling op WB013:

- Als een responsbericht inhoudelijke informatie bevat en afgesproken is dat de deze uitwisseling ondertekend moet worden, dan mag de ontvanger het bericht niet verwerken indien de ondertekening niet valide is. De ontvangende partij moet contact opnemen met de verzender van het responsbericht om het probleem te verhelpen. Hetzelfde bericht nog een keer proberen (retry) mag, maar zal hoogstwaarschijnlijk opnieuw fout gaan. Het is dan zaak deze uitwisseling zo spoedig mogelijk te stoppen tot het probleem opgelost is.

- Als een responsbericht GEEN inhoudelijke informatie bevat (het gaat bijvoorbeeld alleen om een acknowledgement van een push-bericht) en afgesproken is dat de deze uitwisseling ondertekend moet worden, dan moet de ontvanger ervan uitgaan dat het request-bericht verwerkt is. Voer geen retries uit met hetzelfde bericht als het een invalide ondertekening betreft! Er moet dan contact opgenomen worden met de verzender van het responsbericht om het probleem te verhelpen. De ontvangende partij mag in deze situatie het afnemen van de service opschorten zolang het probleem niet verholpen is maar dit is niet noodzakelijk. Edukoppeling wijkt hier dus af op WB013 indien er sprake is van een push-bericht. Hiervoor is gekozen omdat het afkeuren van een ondertekende respons op een push-bericht feitelijk geen verdere betekenis heeft. Dit mag alleen als de acknowledgement GEEN aanvullende gegevens of referentie bevat die weer andere processen kunnen triggeren.

- Als vermoed wordt dat problemen rond de ondertekening veroorzaakt worden door kwaadwillenden dan moet de uitwisseling per direct stopgezet worden.