edustandaard

Edukoppeling

Best practices – WUS

Datum: April 2019

Versie: 0.9

Status: Concept

Inhoudsopgave

1. Inleiding

Zoals een brief in een envelop gaat voor verzending, zo gaat een elektronisch bericht in een digitale verpakking. Digikoppeling is de standaard digitale 'envelop' voor het gestructureerd, beveiligd en betrouwbaar uitwisselen van berichten tussen (semi-)overheidsorganisaties. Edukoppeling bouwt voort op Digikoppeling en is toegespitst op berichtenuitwisseling tussen partijen binnen het onderwijs waarbij met name het gebruik van SaaS-diensten onderkend wordt. Edukoppeling bestaat uit een Architectuur en een Transactiestandaard-profiel gebaseerd op WUS/SOAP. De vigerende versie is te vinden op:
https://www.edustandaard.nl/standaard_afspraken/edukoppeling-transactiestandaard/

NB een tweede profiel gebaseerd op REST is op dit moment in ontwikkeling en zal ter zijner tijd onderdeel uit gaan maken van de Edukoppeling-afspraak. De best practices in deze versie zijn nog volledig gebaseerd op de implementatie van het Edukoppeling WUS-profiel.

1.1. Doel en doelgroep van dit document

Dit document heeft als doel ondersteuning te bieden bij Edukoppeling-implementaties. Het bevat geen voorschriften, maar plaatst deze wel in meer context en bevat op verschillende punten aanvullende informatie.

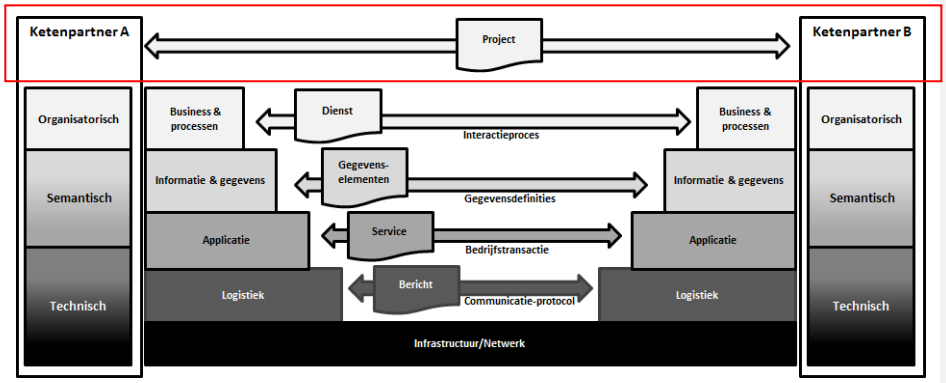
De best practices zijn bedoeld voor medewerkers die bij de (technische) implementatie van Edukoppeling betrokken zijn. Het gaat hierom werknemers (ontwikkelaars, architecten, projectmanagers, informatiemanagers etc.) werkzaam bij softwareleveranciers, bij uitgevers, bij distributeurs, bij uitvoeringsorganisaties als DUO, Kennisnet, Studielink, SBB en de Inspectie van het Onderwijs en, indien van toepassing, ook bij onderwijsinstellingen. De lezer van dit document willen wij vragen om zaken die ontbreken of onduidelijk zijn te melden bij de beheerder van Edukoppeling via info@edustandaard.nl.
Het is ook mogelijk om te participeren in het discussieplatform van Edukoppeling en met andere partijen te discussiëren over de best practices en/of andere zaken:
https://groups.google.com/a/kennisnet.nl/forum/#!forum/edukoppeling

Afkorting	Rol	Taak	Doelgroep
MT	Management	Bevoegdheid om namens organisatie (strategische) besluiten te nemen.	Nee
PL	Projectleiding	Verzorgen van de aansturing van projecten.	Ja, H2
A&D	Analyseren & ontwerpen	Analyseren en ontwerpen van oplossingsrichtingen. Het verbinden van Business aan de IT.	Ja
OT&B	Ontwikkelen, testen en beheer	Ontwikkelt, bouwt en configureert de techniek conform specificaties. Zorgen voor beheer na ingebruikname.	Ja

1.2. Leeswijzer

Hoofdstuk één bevat de inleiding en het doel en toepassingsgebied van dit document. In hoofdstuk twee worden een aantal aspecten toegelicht die betrekking hebben op Edukoppeling projectactiviteiten. In hoofdstuk drie worden de verschillende aspecten van Edukoppeling beschreven. Deze aspecten worden gebruikt voor de verdere indeling van dit document.

2. Aandachtspunten bij projecten



2.1. Afstemming met ketenpartners

2.1.1. Vroegtijdig Programma van Eisen opstellen en afstemmen met ketenpartners

Stel samen met ketenpartners een Programma van Eisen (PvE) op waarin het koppelvlak specifiek en ondubbelzinnig is vastgelegd. Doe dit vroegtijdig in het traject om te voorkomen dat er tijdens de implementatie onderlinge onduidelijkheden zijn. Bespreek dit PvE tot op het laagste niveau in het ketenoverleg, zodat er een volledig en vastgesteld draagvlak is.

2.1.2. Stel vast wat de volwassenheid van de ketenpartner is t.a.v. Edukoppeling

Inventariseer of de ketenpartner reeds beschikt over Edukoppeling implementaties en/of kennis en welke versie dit betreft. Als de ketenpartner hier nog onbekend mee is onderzoek dan welke platformen de ketenpartij gebruikten en in hoeverre hun platformen compliant dan wel flexibel zijn m.b.t. de in Edukoppeling gebruikte standaarden, zoals TLS, WS-Security, WS-Addressing, SOAP 1.1 etc.

2.2. Inrichting verschillende systeemomgevingen

2.2.1. Gebruik een testomgeving om (configuratie) problemen op te lossen

Het kan zijn dat er problemen zijn rond het inrichten van het Edukoppeling transportkanaal. Een (keten)testomgeving omgeving kan het beste worden gebruikt om deze te verhelpen omdat foutmeldingen en logging vaak meer in details geven dan in productie. Verder is men wellicht wat meer flexibel in het doorvoeren van aanpassingen om tot een werkend resultaat te komen.

2.2.2. Houd rekening met verschillen in omgevingen

Zoals hiervoor gesteld kunnen testomgevingen helpen bij inrichtingsvraagstukken. Men dient er wel alert op te zijn dat dan ook in niet-productieomgevingen zaken vaak net anders afgehandeld worden dan in productie. In een testomgeving met testcertificaten kan bijvoorbeeld een CRL revocation server ontbreken. Men moet inzichtelijk hebben hoe de test- en productie omgeving verschillen en hiermee rekening houden bij de overgang.

2.2.3. Test een service vooraf aan de ketentest op de Edukoppeling aspecten

Maak als dienstaanbieder (bijvoorbeeld o.b.v. van SOAPUI[1]) een aantal inhoudelijk juiste testberichten waarmee de transportlagen binnen Edukoppeling (TLS, certificaten, firewalls etc.) getest kunnen worden voordat de software zelf daadwerkelijk klaar is om berichten te verzenden en ontvangen.

Ter ondersteuning van dienstafnemers kunnen dienstaanbieders een (SOAPUI project) toolset aanbieden waarmee dienstafnemers snel technisch kunnen testen. Met de correcte vraagberichten kan het technisch testen scheiden worden van het functionele en kunnen problemen, zoals routering door firewalls en gateways of gebruikte certificaten etc. sneller opgelost worden.

2.2.4. Vroegtijdig certificaten aanvragen

Regel certificaten op tijd en zorg dat deze in de juiste omgeving tijdig geïnstalleerd worden. Als er met versleutelde berichten gewerkt wordt zorg dan dat voortijdig publieke certificaten met ketenpartijen gedeeld is (geldt met name voor dienstaanbieders). Maak indien van toepassing afspraken over de gebruikte infrastructuur om certificaten uit te wisselen. Deze verlopen en er zal dus om een aantal jaar (meestal 3) opnieuw certificaten uitgewisseld moeten worden.

2.2.5. Vroegtijdig identificeren van noodzaak van wijzigingen op firewall

Markeer vroegtijdig eventuele firewall changes. Deze zijn vaak niet moeilijk, maar kosten wel (doorloop-)tijd. De netwerken (en firewalls) zullen https-transport over TCP/IP moeten toestaan.

2.3. Tijdig vaststellen welke versie toegepast moet worden

Met opmerkingen [ER1]: Issue 9

Partijen wisselen binnen een bepaalde keten gegevens met elkaar uit. Er worden afspraken gemaakt over welke gegevens dit zijn en hoe deze uitgewisseld moeten worden. Zowel de gegevens die tussen ketenpartijen uitgewisseld worden als de logistiek kunnen wijzigen. Met het standaardiseren van de logistiek over ketens heen op basis van de Edukoppeling standaard ontstaan er in principe twee onafhankelijke life cycles. Voor een bepaalde service is het dus van belang dat men aangeeft welke versie van Edukoppeling en welke versie van het service contract (de uit te wisselen gegevens) toegepast moet worden.

Ketens kunnen zelf het versiebeheer van de uit te wisselen gegevens inrichten, maar voor de vigerende versie(s) van Edukoppeling is men afhankelijk van het beheerproces van Edustandaard (zie Edukoppeling beheermodel[2]). Het Edustandaard beheerproces bepaalt welke versies de status ‘In Gebruik’ hebben en wanneer een versie de status ‘Einde Ondersteuning’ krijgt. Er zijn maximaal twee Edukoppeling versies met de status ‘In gebruik’. De Edukoppeling standaard is gebaseerd op het Digikoppeling WUS profiel. Voor een Edukoppeling implementatie zijn dus ook de documenten van Digikoppling WUS relevant. Welke documenten dit zijn wordt aangegeven in het Digikoppeling-Overzicht-Actuele-Documentatie-en-Compliance[3] document.

[1] https://www.soapui.org/
[2] https://www.edustandaard.nl/standaard_afspraken/edukoppeling-transactiestandaard/
[3] https://www.logius.nl/diensten/digikoppeling/documentatie

Omdat er verschillende versies van de Edukoppeling standaard kunnen zijn is het verstandig dat een keten expliciet een keuze maakt in de toe te passen Edukoppeling versie. In zijn algemeenheid is het aan te raden om de laatste versie van de standaard te kiezen, maar er kunnen moverende redenen zijn om de eerdere versie te implementeren.

De versie van het service contract bepaald welke gegevens tussen ketenpartijen uitgewisseld worden. De huidige versie van Edukoppeling biedt momenteel enkel de WUS Transactiestandaard en hiermee wordt het contract vormgegeven middels een WSDL[4]. In de WSDL zijn de berichten opgenomen zoals deze over de lijn gaan. De targetnamespace die voor de berichten in de WSDL is gedefinieerd geeft de versie aan. Deze komt ook terug in de namespace van de body van het Request en het Response. Conform DK voorschrift WS008 wordt de WS-Addressing (WSA) Action referentie opgenomen in de WSDL. Het definiëren van een WSA action in de WSDL kan met behulp van de Web Services Addressing 1.0 – Metadata standaard. De WSA Action is een referentie naar een bepaald bericht van een operatie binnen de betreffende WSDL.

De WSDL is het contract voor de gegevensuitwisseling en het is dus van belang dat deze 100% juist is.

2.3.1. Hoe kan de toe te passen versie gecommuniceerd worden naar afnemers?

De keuze rond de toe te passen versie moet kenbaar worden gemaakt aan de afnemende partijen. Dit kan bijvoorbeeld via een Programma van Eisen, of indien beschikbaar via een service register (zie ook het OSR[5]).

2.3.2. Welke versioneringsmethodiek kan gebruikt worden?

Digikoppeling (en Edukoppeling) gebruiken voor documenten de versioneringsmethodiek [documentnaam]_vX.Y.Z. Met vX.Y.Z wordt gerefereerd aan major (X) en minor (Y) releases en (Z) patches (zie ook SEMVER[6]). De huidige versie (april 2019) van de Edukoppeling Transactiestandaard (WUS) is versie 1.3.

Voor de versioneringsmethodiek van het contract (WSDL) wordt verwezen naar het Digikoppeling Best Practices document[7]. Een aantal aspecten hieruit staan hieronder.

1. Er zijn een aantal elementen waaraan een versie aanduiding moet worden toegevoegd. Dit zijn: WSDL/namespace WSDL/Servicenaam WSDL/PortType WSDL/Type(s) (XSD) namespace
2. Er zijn een aantal manieren om de versie van een service aan te duiden. De meest gangbare zijn “Major.Minor”, “Enkelvoudige versie-aanduiding” (bijv. V1) en “YYYY/MM”. Het voorstel is om voor zowel de XSD als de WSDL de Enkelvoudige versie aanduiding te gebruiken (V1 of YYYY/MM).

[4] https://www.w3.org/TR/2001/NOTE-wsdl-20010315
[5] https://www.kennisnet.nl/diensten-voor-de-school/onderwijs-serviceregister-osr/
[6] https://semver.org/
[7] https://www.logius.nl/diensten/digikoppeling/documentatie

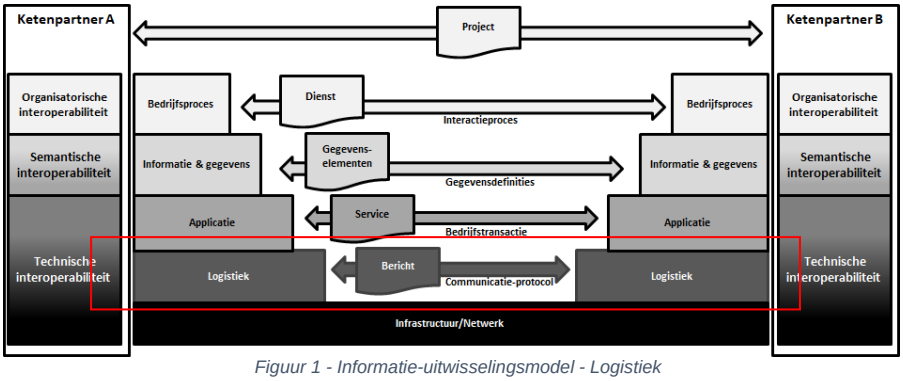
2.3.3. Hoe om te gaan met versie overgangen

Er zijn verschillende manieren om de migratie van de ene versie naar de andere te organiseren. Het belangrijkste onderscheidt is of er een migratiefase wordt toegepast of dat een hele keten gezamenlijk op een bepaald moment over gaat naar de nieuwe versie, de zogenaamde ‘Big Bang’. Bij de toepassing van een migratiefase wordt op een bepaald moment de nieuwe versie geïntroduceerd. Deze variant geeft over het algemeen weinig problemen door introductie van een nieuwe versie, maar de overgang naar de nieuwe versie is wel langer. Verder heeft dit als nadeel dat aanbieders tijdens de overgangsfase zowel de oude als de nieuwe versie moeten ondersteunen. Na de afgesproken termijn wordt de ‘oude’ versie niet meer ondersteund.

Een ‘Big Bang’ migratie biedt over het algemeen een snellere overgang, maar heeft als nadeel dat bij problemen de impact groot kan zijn. Het is bij deze variant wenselijk om een rollback-scenario te ondersteunen. Welke keuze gewenst is verschilt per keten(proces). Indien een keten een bepaalde periode inactief is kunnen ketentesten in deze periode ervoor zorgen dat op het moment dat de activiteit weer start hierbij de nieuwe versie kan worden toegepast.

3. Logistiek

Bij de communicatie tussen ketenpartners kunnen verschillende lagen onderkend worden. Edukoppeling standaardiseert o.a. de logistieke laag (zie Figuur 1 - Informatie-uitwisselingsmodel - Logistiek). We onderkennen hierin met name het transport en beveiliging hiervan.



Figuur 1 - Informatie-uitwisselingsmodel - Logistiek

3.1. Wat biedt TLS

Het TLS protocol biedt een tweetal beveiligingsfuncties, authenticatie en encryptie op transportniveau. Digikoppeling schrijft tweezijdige TLS voor en het gebruik van PKIoverheid certificaten. De PKIoverheid certificaten bevatten een Organisatie Identificerende Nummer (OIN) in het subject serial number van het certificaat. De OIN systematiek wordt beschreven in het Edukoppeling Identificatie en Authenticatie document[8].

Op transportniveau is de partij die wordt geauthenticeerd de partij waarmee de TLS-verbinding tot stand komt. In de context van Edukoppeling kan dit een SaaS leverancier (intermediair) zijn die voor één of meerdere onderwijsinstellingen de gegevensuitwisseling verzorgt. Op transportniveau is het dus niet noodzakelijkerwijs de ‘eigenaar’ van de berichten wiens identiteit wordt gecontroleerd.

TLS kan niet toegepast worden om end-to-end beveiliging uit te voeren. Een deel van end-to-end beveiliging kan worden geregeld met het ondertekenen en versleutelen van berichten. Zie de Edukoppeling Architectuur voor een beschrijving van end-to-end beveiliging.

Zaken die relvant zijn rond het gebruik van PKIoverheidcertificaten wordt toegelicht in Bijlage A – Waar rekening mee te houden bij gebruik van PKI certificaten.

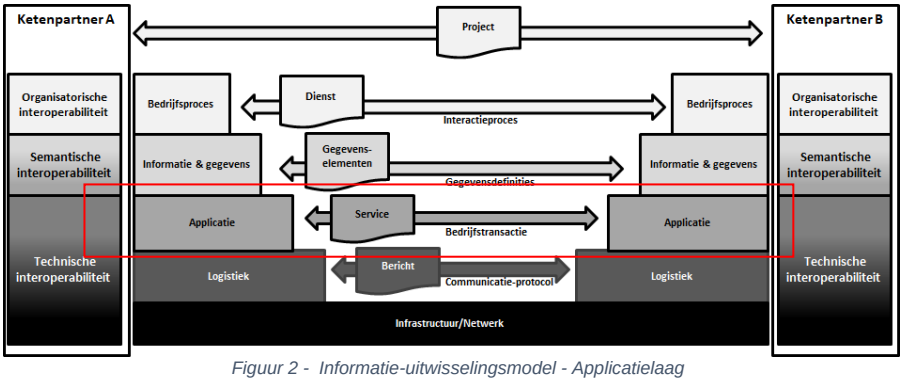
3.2. Het poortnummer kan de service zelf bepalen, maar moet naar afnemers gecommuniceerd worden

Digikoppeling verplicht het gebruik van poort 443. Deze eis is in Edukoppeling los gelaten. Het poortnummer wordt hiermee onderdeel van de logistieke informatie die naar dienstafnemers gecommuniceerd moet worden.

[8] https://www.edustandaard.nl/standaard_afspraken/edukoppeling-transactiestandaard/

4. Applicatielaag

Edukoppeling standaardiseert o.a. aspecten op de applicatielaag (zie Figuur 2). We onderkennen hierin zaken als beveiliging en adressering, etc.



Figuur 2 - Informatie-uitwisselingsmodel - Applicatielaag

4.1. Zorg ervoor dat web service gegevens actueel zijn

Gebruik bijvoorbeeld een serviceregister en richt processen in om de gegevens actueel te houden en zorg ervoor dat verantwoordelijkheden belegd zijn.

4.2. Pas naming conventions toe

Servicenamen moeten uniek zijn binnen een bepaald domein. Dit kan gerealiseerd worden door de toevoeging van domein-specifieke woorden waar nodig. Een te veel vereenvoudigde naam kan zeer verschillende betekenissen hebben in verschillende domeinen. Bij opname in een serviceregister dat meerdere domeinen ondersteund kan dit zeer verwarrend zijn en tot fouten leiden.

Voor de verwerking van de berichten in de SOAP handlers is het wenselijk om elke WSDL een eigen namespace te geven om conflicten tussen de berichten, operaties etc. van verschillende services te voorkomen.

Servicenamen worden vaak gebruikt door implementatie toolkits die bij het verwerken van de WSDL de noodzakelijke softwareobjecten genereren waarbij mogelijk spaties of speciale tekens niet zijn toegestaan. Deze moeten bij voorkeur dan ook niet in de naam van een service voorkomen.

Een servicenaam moet zijn operaties in de juiste context plaatsen. De operatienaam moet de afnemer voldoende informatie verschaffen met betrekking tot het gedrag van de operatie.

4.3. Valideer berichten tegen het XSD schema indien mogelijk

Indien mogelijk valideer de binnenkomende berichten tegen het XSD schema voordat zij worden doorgezet voor verdere verwerking. Het kan zijn dat een bericht niet voldoet aan het schema zoals gedefinieerd door de WSDL en het is wenselijk deze invalide berichten voegtijdig te detecteren. Het valideren van berichten kan als extra stap gezien worden die extra resources vereist. Het is dan ook deels afhankelijk van de systeemomgeving of dit toegepast kan/moet worden. Het wordt sterk aanbevolen om in ieder geval in de test- en acceptatiefase schemavalidatie uit te voeren als men het vertrouwen heeft dat er met de

overgang naar productie geen wijzigingen plaatsvinden die van invloed kunnen zijn op het bericht.

4.4. Waar rekening mee houden bij WS-Addressing

4.4.1. Pas een aanvullende typering voor de MessageId toe

De WSA:MessageId kan volgens de standaard een Uniform Resource Identifier (xs:anyURI) zijn. Partijen kunnen er voor kiezen om hierbij aanvullende voorschriften toe te passen. De wsa:MesssageId kan op basis van een UUID conform IETF RFC 4122 (zie https://www.ietf.org/rfc/rfc4122.txt) gevuld worden. In het bericht wordt de UUID voorzien van de prefix “urn:uuid”.

Bijvoorbeeld

```
…
<soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
<wsa:MessageID soapenv:mustUnderstand="1">
        urn:uuid:1f64216c-ec95-489d-a1c1-0d1ea3656be0
</wsa:MessageID>
</soapenv:Header>
…
```

4.4.2. Hoe om te gaan met verplichte WSA Headers (mustunderstand=1)

Met opmerkingen [ER2]: Issue 13

Verplichte headers WSA headers worden in berichten opgenomen met het attribuut mustunderstand=1. De dienstafnemer en dienstaanbieder moeten verplichte headers kunnen verwerken. Indien in een requestbericht een verplichte header ontbreekt moet de dienstaanbieder de dienstafnemer een foutbericht sturen. Indien in de repsonse een verplichte header ontbreekt, of indien de dienstaanbieder een verplichte header in het request niet kan verwerken, moet de dienstafnemer dit aan de dienstaanbieder kenbaar maken. Zolang partijen niet beide de verplichte WSA headers ondersteunen is er geen sprake van een valide Edukoppeling koppelvlak.

Als een dienstaanbieder een requestbericht ontvangt waarin een verplichte header ontbreekt, wordt als antwoord wordt een SOAP:Fault gestuurd, zie het voorbeeld hieronder (zie voor meer informatie http://www.w3.org/TR/ws-addr-soap/#soapfaults).

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
<wsa:Action> http://www.w3.org/2005/08/addressing/fault</wsa:Action>
<wsa:RelatesTo RelationshipType="http://www.w3.org/2005/08/addressing/reply">
        urn:uuid:7f9f9e8c-be3b-4b45-91b6-ce7c437c6967
</wsa:RelatesTo>
<wsa:To>http://www.intermediairx.nl/services?oin=00000001789455534530 </wsa:To>
<wsa:MessageID>urn:uuid:0d7acc60-6044-4283-a2be-eb4a50ba4c97</wsa:MessageID>
<wsa:From><wsa:Address>
http://www.w3.org/2005/08/addressing/anonymous?oin=000000079876
</wsa:Address></wsa:From>
<wsa:FaultDetail>wsa:From</wsa:FaultDetail>
</soapenv:Header>
<soapenv:Body>
   <soapenv:Fault>
```

```
        <faultcode> wsa:MessageAddressingHeaderRequired </faultcode>
        <faultstring xml:lang="en">
                A required header representing a Message Addressing Property is not present
        < /faultstring>
   </soapenv:Fault>
</soapenv:Body>
</soapenv:Envelope>
```

4.5. Waar rekening mee houden bij ondertekening (2W-be-S profiel)

4.5.1. Toepassen als integriteit en/of onweerlegbaarheid van belang is

Het ondertekenen van een bericht kan worden toegepast indien integriteit en/of onweerlegbaarheid vereist wordt. De ontvanger moet kunnen vaststellen dat het bericht intact en afkomstig van de bron is. Doordat de berichten ook het publieke deel van het certificaat bevatten kan het opgeslagen bericht ook later nog gevalideerd worden. Een aantal relevante Digikoppeling voorschriften voor het ondertekenen zijn (let op: controleer altijd de brondocumentatie):

Digikoppeling WB002
Toepassen van Timestamp in security header met Timestamp Created is verplicht.

Digikoppeling WB004
Ondertekenen van bericht onderdelen SOAP:body, SOAP:headers (WS-Addressing headers en Timestamp) is verplicht bij toepassing van End-to-End beveiliging.

Digikoppeling WB010
Publieke sleutel dat gebruikt is voor het signing proces dient meegeleverd te worden met het bericht via een ‘Direct security token’ reference.

Digikoppeling WB011
Het toepassen van End-to-End beveiliging wordt op serviceniveau aangeduid. Alle operaties en dus berichten (request en response) worden ontsloten volgens één bepaald Digikoppeling profiel.

Digikoppeling WB012
Voor het versleutelen van het responsebericht wordt het certificaat in het requestbericht gebruikt.

Digikoppeling WB013
Indien WS-Security wordt toegepast, is het controleren van de signature door de ontvangende partij verplicht. Indien de validatie mislukt, dient het bericht afgewezen te worden en een foutmelding als antwoord te worden verstuurd.

Digikoppeling WUS wordt alleen voor bevragingen gebruikt en ondersteund in principe geen push-berichten. 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. 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! Er moet 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.

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

Bij push-berichten wijkt Edukoppeling dus op WB013 af. Hiervoor is gekozen omdat het afkeuren van een ondertekende respons op een push-bericht feitelijk geen verdere betekenis heeft. De verwerker van de response dient wel in contact te treden met de dienstaanbieder om herhaling te voorkomen.

WB014
Indien WS-Security wordt toegepast dient het responsebericht de signature van het requestbericht als onderdeel van het SignatureConfirmation element op te nemen (WS-Security 1.1)

4.5.2. Kies een passende timestamp

Met het toepassen van een ondertekening wordt ook de tijdsynchronisatie van de systemen relevant. Een timestamp moet in principe een zo kort mogelijke geldigheidstermijn aangeven. Conform WB002 is het echter niet verplicht een Expires element op te nemen.

4.5.3. Valideer de ondertekening

Bij het toepassen van het profiel met ondertekening (2W-be-S of 2W-be-SE) wordt zowel het request- als het responsbericht ondertekend. Beide partijen valideren de ondertekening bij ontvangst van het bericht (zie opmerking bij WB013). Hierbij wordt tevens de CRL en timestamp gecontroleerd. De timestamp wordt gecontroleerd om vast te stellen of de geldigheidstermijn niet is verlopen, de CRL gebruikt om vast te stellen dat het certificaat niet is ingetrokken. Zie voor meer details rond PKI Bijlage A – Waar rekening mee te houden bij gebruik van PKI certificaten.

4.6. Waar rekening mee houden bij versleuteling (2W-be-SE profiel)

4.6.1. Toepassen als berichtbeveiliging noodzakelijk is

Versleutelen kan worden toegepast voor beveiligd transport. Het bericht gaat mogelijk over niet vertrouwde netwerken en er wordt vereist dat het bericht alleen kan worden ingezien door de bedoelde ontvanger die over de private sleutel beschikt. Edukoppeling versleutelt berichten op transportniveau met behulp van TLS. Berichtenverkeer begint niet vanuit een TLS koppeling. Vaak worden berichten binnen een (intern) netwerk van of naar de TLS koppeling getransporteerd en kan het gewenst zijn om ook tijdens dit transport het bericht beveiligd te hebben. Een aantal relevante Digikoppeling voorschriften voor het versleutelen zijn (let op: controleer altijd de brondocumentatie):

Digikoppeling WB005

Bij toepassen van versleutelen geldt dit voor de volgende bericht onderdelen: SOAP:body

Digikoppeling WB006
Berichten worden eerst ondertekend en vervolgens versleuteld.

Digikoppeling WB012
Voor het versleutelen van het responsebericht wordt het certificaat in het requestbericht gebruikt.

5. Foutafhandeling

Bij het gebruik van een Edukoppeling koppelvlak kunnen fouten optreden. Het Informatie-uitwisselingsmodel (zie **Fout! Verwijzingsbron niet gevonden.**) geeft aan dat fouten zich op verschillende lagen kunnen voordoen, maar ook veroorzaakt kunnen worden door de dienstaanbieder of dienstafnemer. Het is echter alleen de dienstaanbieder die de afweging kan maken of en hoe hij de client over een fout wil informeren. Het is afhankelijk van de situatie (fout) hoe hierover gecommuniceerd wordt.

5.1. HTTP header

Het type fout bepaald de HTTP status code. Conform het WS-I basic profile (http://ws-i.org/profiles/basicprofile-1.2-2010-11-09.html) worden de HTTP 4xx status codes bij de respons gebruikt om één van de volgende fouten aan de dienstafnemer door te geven:

1. "400 Bad Request", HTTP Request message is malformed.
2. “401 Unauthorized”, HTTP Request requires authorization
3. “405 Method not Allowed" Request message's method is not "POST"
4. "415 Unsupported Media Type" Request message's Content-Type header field-value is not permitted by its WSDL description

Overige fouten worden gecommuniceerd met een SOAP Fault. Hiervoor wordt de HTTP status code 500 "Internal Server Error" gebruikt.

5.2. SOAP Faults

Een SOAP Fault bestaat uit de volgende elementen:

- faultcode
- faultstring
- faultactor
- faultdetail

faultcodes
SOAP schrijft een aantal faultcodes voor welke in de respons gebruikt moeten worden, dit zijn:

1. VersionMismatch: Ter indicatie dat de namespace van het SOAP Envelope element niet conform SOAP specificatie is.
2. MustUnderstand: Ter indicatie dat de dienstaanbieder niet in staat is om een verplicht SOAP Header element (value of "1") te verwerken. In de Edukopeling Transactiestandaard staan de WS-Addressing headers die verplicht zijn in de request berichten en door de dienstaanbieder verwerkt moeten kunnen worden, Indien een verplichte Edukoppeling header niet verwerkt kan worden wordt dit met de Mustunderstand faultcode gecommuniceerd. De betreffende foutcode uit de tabel in de Transactiestandaard wordt aan de foutcode toegevoegd (mustUnderstand.<Edukoppeling foutcode>).
3. Client: Ter indicatie dat het request niet van het juiste formaat is of onjuiste informatie bevat. Het bericht moet niet zonder wijziging opnieuw gestuurd worden. Indien de fout betrekking heeft op een Edukoppeling eis dan wordt de betreffende foutcode uit de tabel in de Transactiestandaaaan de foutcode toegevoegd (Client.<Edukoppeling foutcode>).
4. Server: Ter indicatie dat het bericht niet verwerkt kan worden om redenen die niet aan de inhoud van het bericht te relateren zijn.

faultstring
Indien de fout betrekking heeft op een Edukoppeling voorschrift dan wordt dit element gevuld met de omschrijving van de betreffende Edukoppeling foutcode (zie tabel in Transactiestandaard). In andere gevallen kan hierin een eigen service specifieke beschrijving van de fout opgenomen worden. Indien de faultcode Client is dan moet hierin informatie opgenomen worden die de dienstafnemer kan gebruiken om een correct request te sturen.

faultactor
Indicatie van de bron van het SOAP Fault bericht. Dit is de dienstaanbieder indien er geen sprake van een intermediairs is. Een SOAP actor wordt aangeduid met een URI.

faultdetail
Wordt alleen gebruikt om fouten binnen de SOAP Body aan te duiden.

5.3. Best practices foutafhandeling

De onderstaande afspraken maken voor het definiëren van de foutsituaties gebruik van de foutcategorieën zoals gedefinieerd in de Edukoppeling Architectuur[9] en de HTTP statuscodes zoals gedefinieerd in de SOAP standaard en het WS-I basic profile 1.2[10].

FOUTSITUATIE	HTTP CODE	FORMAAT
SOAP vraagbericht syntax fout (Cat. A)	500*	SOAP Fault Message
SOAP vraagbericht functionele fout (Cat. D)	500*	SOAP Fault Message
Interne server fout (Cat. B)	500*	SOAP Fault Message
Interne server fout (Cat. C)	5xx	HTTP
Client fout (Cat. A)	4xx	HTTP

** SOAP 1.1 requires that SOAP Fault can only be returned with HTTP 500 "Internal Server Error" code.*

- De HTTP statuscode geeft een indicatie of een requestbericht succesvol verwerkt is of niet en of de fout bij de client of server lag:
  - 5xx Server fout: wordt gebruikt om met een SOAP Fault een syntax fout (Cat A), een functionele fout (Cat D) of een service gesloten fout (Cat B) te communiceren.
  - 4xx Client fout: wordt gebruikt bij Cat. A fouten indien de fout op HTTP niveau plaatsvindt, bijvoorbeeld method not allowed (405) or bad requests (404);
  - 5xx Server fout: wordt gebruikt bij Cat. C fouten time-out (408)
- De HTTP statuscode wordt gebruikt voor de logging van fouten (fouten worden NIET met HTTP statuscode 2xx gecommuniceerd).
- Een SOAP Fault wordt met een HTTP statuscode 500 gecommuniceerd met een SOAP faultcode die aangeeft of de fout bij de client of server lag.
  - Een SOAP Fault met faultcode = 'Client' wordt gebruikt om de client te informeren over wat aan het request veranderd moet worden voordat deze opnieuw verstuurd wordt. Dit kunnen Syntax fouten zijn en komen met name voor in de testfase.
  - Een SOAP Fault met faultcode = 'Server' wordt gebruikt om Service gesloten fouten aan de client te communiceren. Of het betreft Functionele fouten die bijvoorbeeld door een ander proces zijn veroorzaakt. Bijvoorbeeld bij het specificeren is er niet

9 https://www.edustandaard.nl/standaard_afspraken/edukoppeling-transactiestandaard/
10 http://ws-i.org/profiles/basicprofile-1.2-2010-11-09.html

voldoende voorraad beschikbaar. Deze fouten komen met name voor in de productiefase.

- In de SOAP Fault response wordt de WSA:Action header gevuld waarvoor het volgende geldt:
  - http://www.w3.org/2005/08/addressing/fault gebruiken als het om WS-Addressing fouten gaat.
  - http://www.w3.org/2005/08/addressing/soap/fault gebruiken als het om SOAP version mismatch en must understand fouten gaat.
  - In overige gevallen wordt de WSA:Action gevuld met de wsa:action zoals gedefinieerd in de WSDL.
- In de WSA:RelatesTo header wordt de WSA:MessageId van het request opgenomen.
- Als de WSA:From in zijn geheel het betreffende OIN in het request ontbreekt dan mag in de SOAPFault een WSA:To zonder OIN gestuurd worden. 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).
- Indien het request headers bevat die geen onderdeel zijn van de standaard wordt een SOAP Fault met foutcode 10 (Andere headers) teruggestuurd. Het is van belang dat het gebruik van andere headers bij de beheerder van Edukoppeling bekend wordt gemaakt. Dit om vast te kunnen stellen of deze headerinformatie van belang is voor de doorontwikkeling van de standaard.
-

Met opmerkingen [ER3]: Issue 30

Met opmerkingen [ER4]: Issue 31

Met opmerkingen [ER5]: Issue 32

6. Bijlage A – Waar rekening mee te houden bij gebruik van PKI certificaten

Conform Digikoppeling schrijft Edukoppeling alleen het gebruik van PKIoverheid certificaten toe voor TLS en het ondertekenen en versleutelen van berichten. Bij het testen kan in testomgevingen eventueel nog wel een DUO ODOC certificaat toegepast worden.

6.1. Certificaat moet verwijzen naar een valide CA

Een certificaat wordt uitgegeven door een certificaatautoriteit (CA, zie ook CSP en TSP). De CA waarborgt de integriteit en authenticiteit van het certificaat en toetst of de afnemer een bestaande en legale organisatie is.

Een CA heeft een eigen certificaat dat ondertekend is met het PKIoverheid domeincertificaat (Domein Organisatie Services-G3 / Domein Organisatie-G2) en kan pas vertrouwd worden als dit daadwerkelijk het geval is. De certificaten die een CA uitgeeft zijn met dit CA certificaat ondertekend. Hiermee is feitelijk elk uitgegeven certificaat onderdeel van een hiërarchie van certificaten. Deze “chain of trust” moet bij de gebruikte systemen vertrouwd worden. Met het PKIoverheid stamcertificaat, domeincertificaat en die van de CA in de trust store kan de echtheid van een PKIoverheid certificaat dat een partij bij communicatie, ondertekening of ondertekening gebruikt, gecontroleerd worden.

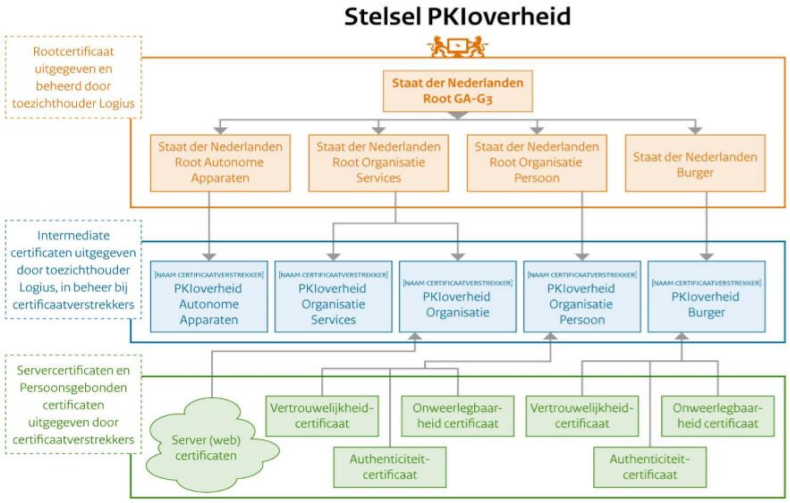
Een overzicht van de PKIoverheid CA’s is te vinden op https://www.pkioverheid.nl/.

6.2. Valideer de hiërarchie van het certificaat

Met opmerkingen [ER6]: Issue 35

Op dit moment zijn er meerdere certificaathiërarchieën van PKIoverheid (G1,G2 en G3). Na verloop van tijd zijn steeds sterkere algoritmes of andere functionaliteiten nodig om de betrouwbaarheid van certificaten te kunnen garanderen. Alle certificaten binnen eenzelfde hiërarchie zijn gebaseerd op hetzelfde algoritme. Zie voor meer details Digikoppeling-Gebruik-en-achtergrond-certificaten[11]. Om foutmeldingen te voorkomen bij machine-to-machine communicatie, moet de gehele certificaatketen van eindgebruikerscertificaat tot aan het stamcertificaat gevalideerd kunnen worden. Deze hiërarchieën zijn te raadplegen op de website van PKIoverheid[12] (zie ook Figuur 3).

[11] https://www.logius.nl/diensten/digikoppeling/documentatie
[12] https://www.logius.nl/diensten/pkioverheid/hoe-werkt-het



Figuur 3 - PKIoverheid

6.2.1. Public en Private Root certificaten

Een PKIoverheid services servercertificaat komt in twee soorten, een Public Root en een Private Root certificaat (zie PKIoverheid[13]). Servercertificaten zijn geschikt voor de beveiliging van verkeer tussen systemen en verkeer naar/van websites. Voor beide type certificaten geldt dat ze aan de eisen van PKIoverheid voldoen, veilig beheerd worden en een audit ondergaan door een derde, onafhankelijke partij. De certificaten verschillen echter op twee punten, de geldigheidsduur en de toepasbaarheid van het certificaat. Digikoppeling en dus ook Edukoppeling staat het gebruik van beide soorten toe. Beide hiërarchieën moeten dus vertrouwd worden.

6.2.2. Hoe gaat de validatie van de hiërarchie van het certificaat in zijn werk?

Met opmerkingen [ER7]: Issue 35

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 algemeen de public root certificaten al standaard opgenomen. Het is waarschijnlijk dat opname van de Private Root certificaten in de truststore extra beheer vereist.

6.3. Controleer of een certificaat is ingetrokken

Met opmerkingen [ER8]: Issue 34

Of een certificaat is ingetrokken kan worden vastgesteld met een Certificate Revocation List (CRL). De CRL is zowel relevant voor het TLS koppelvlak als bij ondertekende en/of versleutelde berichten.

Partijen kunnen bij verschillende Trust Service Providers (TSP's) PKIoverheid certificaten afnemen, elke TSP stelt (net als PKIoverheid voor de stamcertificaten op https://crl.pkioverheid.nl/) een CRL beschikbaar met ingetrokken certificaten. Partijen moeten vertrouwde certificaten controleren tegen de CRL van de TSP die deze heeft uitgegeven. Het

[13] https://www.logius.nl/diensten/pkioverheid/verschil-public-en-private

certificaat zelf bevat de informatie die nodig is om de locatie van de CRL van de TSP te bepalen (CRL Distribution Point).

De TSP draagt de verantwoordelijkheid dat de CRL aan het Programma van Eisen van PKIoverheid voldoet en ook beschikbaar is. TSP's stellen periodiek een nieuwe CRL beschikbaar. De geldigheid van de CRL overlapt de duur tussen één of meer updates. Deze langere geldigheid moet eventuele tijdelijke storingen kunnen overbruggen. Als de CRL van de TSP of PKIoverheid toch niet beschikbaar is via het internet terwijl de vorige versie is verlopen kan er in principe niet voldaan kan worden aan de voorgeschreven beveiligingsmaatregelen. De verantwoordelijkheid om wellicht de gegevensuitwisseling te staken ligt bij de keten(partij). Het is verder hoogst onwaarschijnlijk dat de PKIo of TSP CRL's niet tijdig beschikbaar zullen zijn.

De CRLs van de root certificate van PKIoverheid staan op https://crl.pkioverheid.nl/

6.4. Laat het certificaat tijdig intrekken

Er zijn verschillende TSP's die hier over informeren. Het laten intrekken van een certificaat is vaak gratis. Vaak is dit in de volgende situaties vereist:

- Uw privésleutel (private key) is corrupt (bijvoorbeeld beschadigd of geïnfecteerd).
- Uw privésleutel is gecompromitteerd (niet meer geheim).
- U weet het wachtwoord of de PIN-code van uw privésleutel niet meer.
- Uw privésleutel is verloren geraakt bij het upgraden of crashen van de server.
- Bij installatie is er een 'private key mismatch'.
- Bij installatie is er geen 'pending request' in de server.
- Bij installatie blijkt dat er een certificaat voor een onjuiste CN-naam (Common Name) is aangevraagd.
- Uw certificaat bevat onjuiste informatie.
- Uw certificaat werkt niet goed.

6.5. Controleer of het OIN aanwezig is in het certificaat (Subject.Serialnumber)

Partijen kunnen worden geïdentificeerd op basis van het OIN. Voor partijen met een registratie in het Handelsregister (HR) kan het OIN op het kvk-nummer gebaseerd worden. Het OIN van een onderwijsinstelling wordt gebaseerd op het BRIN.

Het OIN van een bepaalde organisatie wordt opgenomen in het certificaat dat een tekenbevoegd persoon namens die organisatie bij een Trust Service Provider[14] (TSP) / Certificate Service Provider (CSP) heeft aangevraagd. Bij gegevensuitwisseling kan worden getoetst of het OIN in het certificaat is opgenomen. Door gebruik van PKI certificaten en toepassing van tweezijdige TLS en/of ondertekening van berichten, beschikken beide partijen over elkaars identiteit welke tevens geauthentiseerd is door een TSP. Hierna kan op basis van onder meer het OIN bepaald worden of de partij geautoriseerd is.

6.6. Controleer de Common Name (CN) met domein gebruikte service endpoint

Het is gewenst om de CN uit het certificaat van de dienstaanbieder te controleren tegen de domeinnaam van het gebruikte service endpoint. Het Programma van Eisen (PvE) van PKIoverheid vereist opname van een Fully Qualified Domain Name (FQDN) in de CN. Het gebruik van een lokaal domein of uitsluitend een hostnaam wordt niet toegestaan. Het

[14] Een overzicht van TSP's is te vinden op https://www.pkioverheid.nl/

gebruik van enkel een hostnaam wordt sinds 1 november 2015 niet meer toegestaan. Met de eis voor het toepassen van een FQDN is ook het gebruik van wildcard certificaten niet toegestaan. Deze bieden niet voldoende vertrouwen.

6.7. Controleer de Subject Alternative Names bij service met een SAN certificaat

Controle van het CN van het certificaat tegen het endpoint van de web service is mogelijk niet voldoende. Een dienstaanbieder gebruikt mogelijk één certificaat om web services op meerdere subdomeinen te beveiligen. In dit certificaat zijn dan de verschillende endpoints als Subject Alternative Names opgenomen (SAN certificaat). De dienstafnemer controleert of er een SAN voor het endpoint is opgenomen. Bij gebruik van een SAN certificaat is de spreidingskans van de privésleutel groter dan bij een certificaat zonder SAN[15].

15 https://developers.wiki.kennisnet.nl/index.php?title=OSO:2018/beveiliging/certificaten_webservice#Type_certificaat

7. Bijlage B – Patronen bij gegevensuitwisseling

7.1. Push vs Pull berichtuitwisseling

Met opmerkingen [ER9]: Actiepunt 77

7.2. Granulariteit berichten

7.3. Routering en intermediairs

Met opmerkingen [ER10]: Issue 23