Implementatie-afspraken document

Koppelvlak-specificatie synchrone bevraging

|  |  |
| --- | --- |
| Datum: | 11 juli 2018 |
| Betreft: | Implementatie-afspraken koppelvlak-specificatie **synchrone bevraging** |

**Type uitwisseling:** Synchrone bevraging

**Toegepaste standaarden:** SuwiML Transactiestandaard versie 4.0

SuwiML Berichtstandaard v.2.2

**FWI:** FWI-v0203

**Toepassingsgebied:** Suwinet Inkijk, Suwinet Inlezen

**SOAP Header: Adressering**

**WS-Addressing elementen voor een synchroon Request**

In deze versie van de Transactiestandaard gebruiken we de volgende elementen in de SOAP Headers: <wsa:MessageID>, <wsa:Action>, <wsa:From>, <wsa:To> en <wsa:RelatesTo>.

De overige elementen zijn optioneel. Met een verwijzing in de WSDL naar het regel: <wsaw:UsingAddressing wsdl:required="true"/>, hoeven de optionele elementen niet expliciet te worden uitgeschreven. Als de toolkit de optionele WSA-elementen automatisch genereert, die niet onderdrukt kunnen worden, dan gelden de voorschriften conform Digikoppeling. Hierbij geldt wel de beperking dat de waarde voor deze elementen het routeringsmechanisme niet verstoort.

| **Tag** | **Verplichtingen: V/C/O** | **Vulling** | **Omschrijving** | **Bron** |
| --- | --- | --- | --- | --- |
| <wsa:MessageID> | Verplicht | URI ter identificatie van een enkel request[: http://afzender/](http://afzender/) someuniquestring | Unieke identificatie van het bericht t.b.v. traceerbaarheid. | Te bepalen door de afzender |
| <wsa:From> | Verplicht | URI van de vragende webservice of applicatie en het (sub-)OIN van de afnemer: https://applicatie.afnemer.nl/dienst?oin=xxxxxxxxxxxxxxxxxxxx | Autorisatie van de requester inclusief (sub)OIN | Het volledige adres van de oorspronkelijk webservice die het request verstuurd |
| <wsa:To> | Verplicht | URI ter identifcatie van het endpoint van de webservice:  https://suwibroker-productie.suwinet.nl/suwibroker/soap/naamservice-v0100?oin=xxxxxxxxxxxxxxxxxxxx | Endpoint van het request inclusief (sub)OIN | wsdl:definitions / wsdl:service/ wsdl:port/  soap:address/  @location |
| <wsa:Action> | Verplicht | URI ter identificatie van het input-bericht zoals gedefinieerd in de WSDL | Unieke identificatie zoals bepaald in de WSDL voor het Request, Response en Fout. | wsdl:definitions / wsdl:portType /  wsdl:operation / wsdl:input /  [@wsaw:Action](mailto:@wsaw:Action) |

De URI van een webservice/applicatie is altijd het adres van webservice/applicatie, die het SuwiML-koppelvlak implementeert. Dit is nooit het adres een transparant tussenstation.

De <wsa:From> bevat twee elementen. Een URI (adres) en een OIN. Het adres is altijd van de locatie waar het bericht ondertekend is. Dit kan het adres zijn van de applicatie/webservice, een niet transparant tussenstation of het adres van een SAAS-applicatie.

WS-Addressing elementen voor een synchroon Response op een synchroon Request

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tag** | **Verplichtingen: V/C/O** | **Vulling** | **Omschrijving** | **Bron** |
| <wsa:MessageID> | Verplicht | URI ter identificatie van een enkel response:<http://beantwoorder/someother> uniquestring | Unieke identificatie van het bericht t.b.v. traceerbaarheid. | Te bepalen door de zender van het  Response |
| <wsa:From> | Verplicht | URI van de antwoordende webservice of applicatie: <https://suwibroker-productie.suwinet.nl/suwibroker/soap/naamservice-v0100> ?oin=xxxxxxxxxxxxxxxxxxxx | t.b.v. logging. | Het volledige adres van de oorspronkelijk webservice die het response verstuurd (wsa:To uit request) |
| <wsa:To> | Verplicht | URI ter identifcatie van het endpoint van de webservice en het (sub-)OIN van de afnemer?:  https://applicatie.afnemer.nl/dienst?oin=xxxxxxxxxxxxxxxxxxxx | t.b.v. logging | Wordt gevuld met het adres uit de From van het request |
| <wsa:Action> | Verplicht | URI ter identificatie van het output-bericht zoals gedefinieerd in de WSDL | Unieke identificatie zoals bepaald in de WSDL voor het Request, Response en Fout. | wsdl:definitions / wsdl:portType /  wsdl:operation / wsdl:output /  [@wsaw:Action](mailto:@wsaw:Action) |
| <wsa:RelatesTo> | Verplicht | URI ter identificatie van het bijbehorende request:<http://afzender/someuniquestri>ng | Een verwijzing naar de Identificatie van het bericht uit het bijbehorende Request | <wsa:MessageId> uit het Request |

**Gebruik OIN: Identificatie, authenticatie en autorisatie**

Het Organisatie Identificatienummer (OIN) is de basis voor het identificatieproces. Het Organisatie Identificatienummer (OIN) betreft het nummer van de “hoofd” organisatie. Bijvoorbeeld Gemeente Amsterdam.

Voor de gegevensuitwisseling binnen de Suwiketen is echter niet altijd de “hoofd” organisatie die geautoriseerd moet worden, maar bijvoorbeeld een bedrijfsonderdeel. Bijvoorbeeld de gemeentelijke sociale dienst van Amsterdam. Hiervoor heeft Logius de sub-OIN’s geïntroduceerd. En wordt meer fijnmazig autoriseren op basis van sub-OIN mogelijk gemaakt. De Gemeente Amsterdam kan bij Logius een sub-OIN voor de sociale dienst aanvragen. Ook is het mogelijk om voor voorzieningen of applicaties sub-OIN’s aan te vragen (Zie www.logius.nl voor meer informatie).

In het aansluitproces van een afnemer wordt ook definitief vastgesteld voor welk situatie een sub-OIN moet worden aangevraagd.

**SOAP Header: Signature**

Voor de gegevensuitwisseling tussen 2 webservices maken we gebruik van het Digikoppeling-profiel 2W-BE-S. 2W= 2 weg (dubbelzijdige) TLS-verbinding, BE= Best Effort, S=Signed.

Dit betekent dat de verzendende partij het bericht signeert met zijn private (geheime) sleutel, de ontvangende partij ontcijfert de elektronische handtekening (signing) met de publieke sleutel van de verzendende partij en de verbinding vindt plaats op basis van een TLS-PKI-Overheid certificaat. Dit zal moeten gebeuren op de wijze die Digikoppeling voor dit profiel voorschrijft.

Ten behoeve van het ondertekenen van onderdelen in berichten wordt in de WSDL gebruik gemaakt van WS-Policy. Hierin wordt beschreven welke onderdelen van het bericht: SOAP-Header en/of SOAP-Body gesigneerd worden.

Voor de wsa-elementen, als onderdeel van de geldt dat deze ook een ondertekend moeten worden. De SOAP-body wordt als geheel ondertekend.

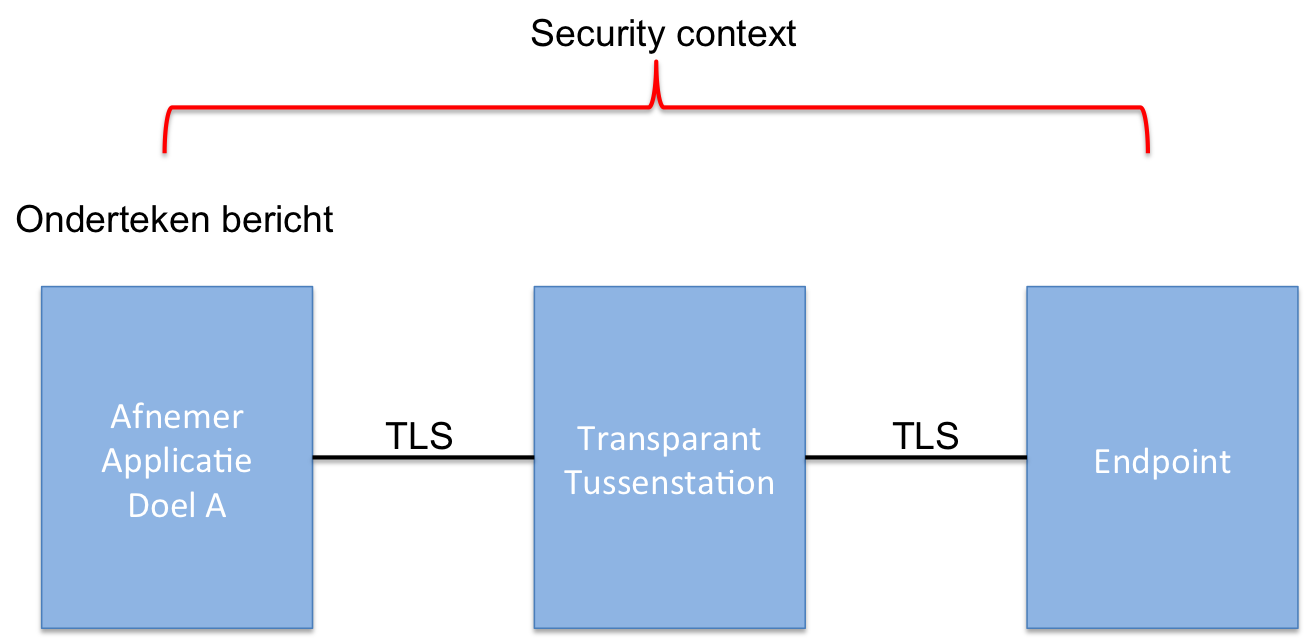
Met een verwijzing in de WSDL naar het regel: <wsp:UsingPolicy wsdl:required="true"/>, hoeven de optionele elementen niet expliciet te worden uitgeschreven. Als de toolkit de optionele elementen automatisch genereert, die niet onderdrukt kunnen worden, dan gelden de voorschriften conform Digikoppeling.

Bij het onderteken van berichten moet rekening gehouden worden met toevoegen van timestamps. Zie hierover de richtlijnen van Digikoppeling.

**Uitwerking 2W-be-S met 1 of meer tussenstations (paragraaf 5.3.4 uit Transactiestandaard 4.0)**

Bij het aansluiten van een afnemer zal duidelijk moeten worden om welke situatie het gaat.

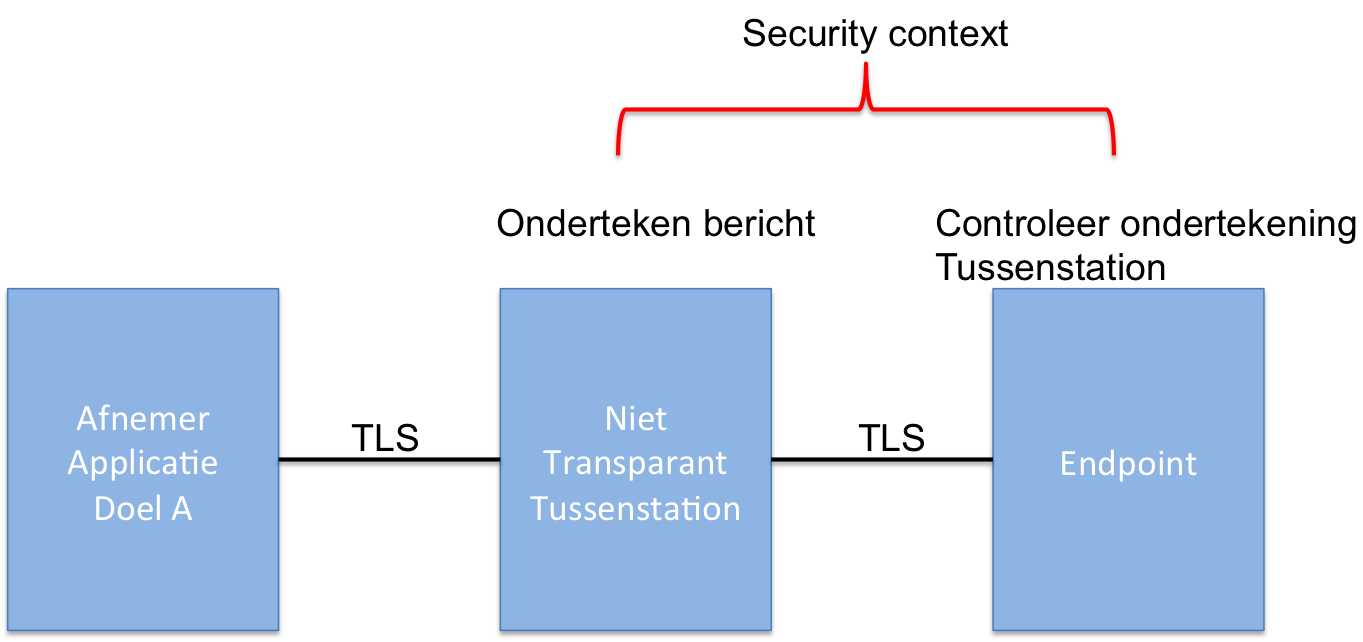
De 2-zijdige TLS verbinding in onderdeel van de beschrijving van deze situatie. En als er meer dan één tussenstation aanwezig is moet elke verbinding van de afnemer tot en met endpoint voorzien worden van TLS. De verbinding wordt altijd tot stand gebracht met PKI-overheid certificaten.



Afbeelding 10 Afnemer met transparant tussenstation

Kenmerken verbinding met een transparant tussenstation:

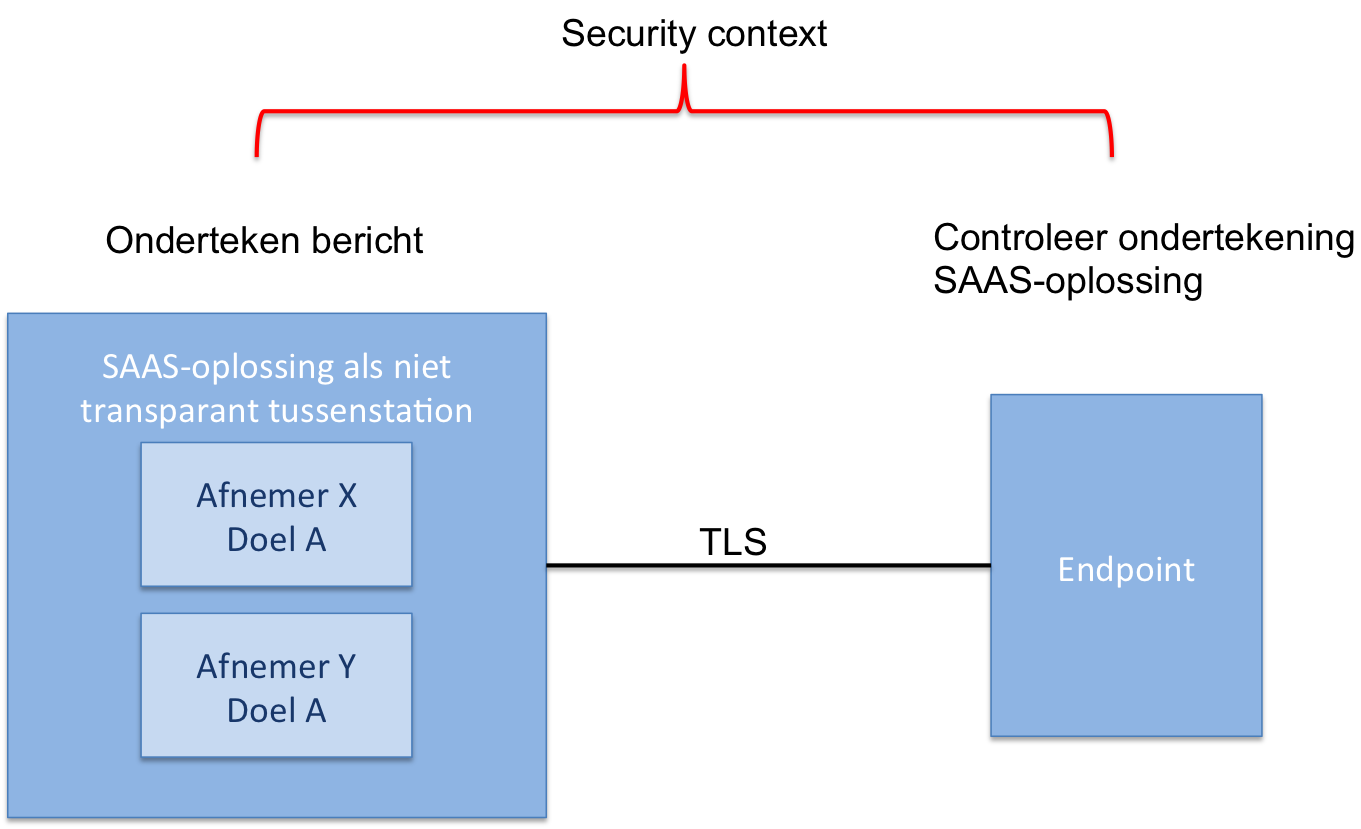
* De applicatie/webservice ondertekent het bericht.
* Elke afzonderlijke afnemer heeft zijn eigen identiteit in de vorm van een sub-OIN.
* Van de afnemer tot aan het endpoint worden berichten uitgewisseld op basis van SuwiML.
* Het transparant tussenstation routeert het bericht naar het endpoint of evetueel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



Afbeelding 11 Afnemer met niet transparant tussenstation

Kenmerken verbinding met een niet transparant tussenstation:

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



Afbeelding 12 SAAS-oplossing als tussenstation

Ander dan een de niet transparante tussenstation bevat een SAAS-oplossing naast de webservices om berichten op te vragen ook meer business-functies. Bijvoorbeeld een applicatie die door een marktpartij via een private cloud aan meer dan één afnemer wordt aangeboden. Of denk aan een constructie waarbij meer gemeenten 1 pakket gebruiken.

Kenmerken verbinding met een SAAS-oplossing:

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