Edukoppeling

Best practices

Edustandaard

Datum: Juli 2017

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. De vigerende versie is Edukoppeling 1.2.

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. Het best practices document zal van tijd tot tijd aangevuld/aangepast worden onder op basis van de feedback die wordt geleverd en/of ervaringen uit implementaties.
(https://www.edustandaard.nl/standaard_afspraken/edukoppeling-transactiestandaard/)

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 1 bevat de inleiding en het doel en toepassingsgebied van dit document. In hoofdstuk 2 worden een aantal aspecten toegelicht die betrekking hebben op Edukoppeling projectactiviteiten. In hoofdstuk 3 worden de verschillende aspecten van Edukoppeling beschreven. Deze aspecten worden gebruikt voor de verdere indeling van dit document.

1.3. Historie

Versie	Auteur	Opmerking
0.1	Edustandaard	Initiële versie (niet gedistribueerd)
juli 2017	Edustandaard / DUO	Mede ook vanuit DUO aanvulling op verschillende aspecten.

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.

2.1.3. Stel vast wat de toe te passen versie van Edukoppeling wordt

Net als met de meeste standaarden wordt ook Edukoppeling actief beheerd en doorontwikkeld. Hierdoor ontstaan er meerdere versies. Vanuit de beheerorganisatie (Edustandaard) wordt er op gestuurd om maximaal 2 (major/medior) versies te ondersteunen. De betreffende Edustandaard-werkgroep bepaalt welke versies er ondersteund worden en wanneer een versie uitgefaseerd wordt. De werkgroepleden vertegenwoordigen verschillende partijen uit het onderwijs waaronder brancheorganisaties en publieke uitvoeringsorganisaties en zijn betrokken in 1 of meerdere ketens in het onderwijs.

Omdat er verschillende versies van de standaard zijn is het verstandig dat een bepaalde 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 keuze wordt opgenomen in het PvE.

2.1.4. Zorg ervoor dat passende informatie beschikbaar is

Beschrijf de service middels een WSDL en XSD en geef voorbeeld (HTTP) berichten zoals ze over de lijn gaan. Zorg dat deze 100% juist zijn.

Maak als dienstaanbieder een (SOAP-UI[1]) project die dienstafnemers kunnen gebruiken om snel technisch correcte berichten uit te kunnen wisselen. Hiermee kan het functioneel en technisch testen scheiden worden en kunnen andere mogelijke problemen, zoals routering door firewalls en gateways of gebruikte certificaten etc. sneller opgelost worden.

[1] https://www.soapui.org/

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) 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.

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.

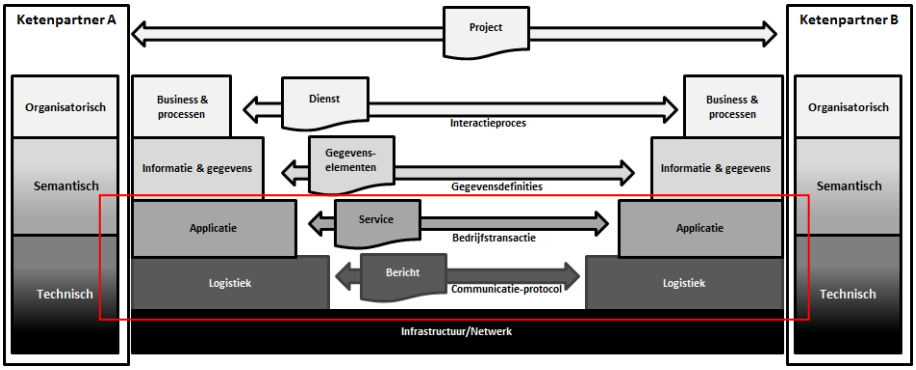
2.2.5. Vroegtijdig identificeren van noodzaak van wijzigingen op firewall

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.

3. Aandachtsgebieden rond de techniek

Edukoppeling is de logistieke laag voor standaardisatie van communicatie tussen systemen op basis van web service standaarden. Bij de communicatie tussen ketenpartners kunnen verschillende lagen onderkend worden (zie Figuur 1). Edukoppeling standaardiseert aspecten op zowel de applicatielaag als de logistieke laag. We onderkennen hierin zaken als het transport, messaging en adressering, etc. De technische best practices hebben betrekking op de volgende lagen:

1. Applicatielaag (Service register, WSDL, SOAP, WS-Addressing en WS-Security)
2. Logistieke laag (HTTP(S), TLS, PKI)
3. Infrastructuur (Internet)



Figuur 1 - Opbouw Edukoppeling

3.1. Applicatielaag

3.1.1. 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.

3.1.2. 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 consumeren van de WSDL de noodzakelijke objecten genereren waarbij mogelijk spaties of speciale tekens niet zijn toegestaan. Deze moeten bij voorkeur dan ook niet in de naam van een service voorkomen.

Met opmerkingen [BD1]: Verwerken?

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.

3.1.3. 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.

3.1.4. Houd bij het ondertekenen rekening met de volgende aspecten

Toepassen als onweerlegbaarheid van belang is
Het ondertekenen van een bericht kan worden toegepast indien 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.

Maak aanvullende afspraken over de te ondertekenen elementen
Digikoppeling WB004 stelt dat er verschillende elementen van het bericht ondertekend moeten worden, maar specificeert niet of deze afzonderlijk of als geheel ondertekend moeten worden. Platformen gaan hier helaas verschillend mee om en dit vereist mogelijk bilaterale afstemming.

Zowel het PKIoverheid als het ODOC certificaat kan gebruikt worden
Edukoppeling staat zowel het gebruik van PKIoverheid als ODOC certificaten (uitgegeven door DUO voor gebruik in het onderwijsdomein) toe voor het ondertekenen van berichten. De ontvanger van een ondertekend bericht dient dus beide typen certificaten te vertrouwen.

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.

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. 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.

3.1.5. Houd bij het versleutelen rekening met de volgende aspecten

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.

3.1.6. 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>
…
```

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

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>
```

3.1.8. Foutafhandeling

Er worden verschillende categorieën fouten onderkend, zie hiervoor de Edukoppeling Architectuur. Syntaxfouten hebben betrekking op de zaken die Edukoppeling voorschrijft. Dit kan zijn indien een partij niet geautoriseerd is, maar ook indien een bericht afwijkt van het betreffende schema. Deze fouten worden gecommuniceerd middels een SOAPFault bericht.

Een andere categorie fouten zijn de functionele fouten. Deze fouten staan los van de Edukoppeling standaard. Functionele resultaten kunnen worden teruggekoppeld als onderdeel van de response in het responsebericht.

3.2. Logistieke laag

3.2.1. Wat biedt TLS

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.

3.2.2. Waar rekening mee te houden bij gebruik PKI certificaten

In Digikoppeling is ervoor gekozen om PKIoverheid certificaten te gebruiken op het niveau van het communicatiekanaal (TLS) en de ondertekening en/of versleuteling van berichten. Edukoppeling ondersteunt naast deze PKIoverheid certificaten tevens het gebruik van DUO ODOC[2] certificaten toe.

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.

[2] https://zakelijk.duo.nl/cps/

Een overzicht van de PKIoverheid CA's is te vinden op https://www.pkioverheid.nl/. De DUO ODOC hiërarchie kan bij DUO opgevraagd worden.

Controleer of een certificaat is ingetrokken
Partijen kunnen bij verschillende 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. Voor ODOC certificaten stelt DUO een eigen CRL beschikbaar, ook voor het stamcertificaat, op http://zakelijk.duo.nl/crl/. Partijen moeten vertrouwde certificaten controleren tegen de CRL van de CSP die deze heeft uitgegeven.

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.

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 en wordt opgenomen in een ODOC-certificaat.

Het OIN van een bepaalde organisatie wordt opgenomen in het certificaat dat een tekenbevoegd persoon namens die organisatie bij een Trust Service Provider[3] (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 CSP. Hierna kan op basis van onder meer het OIN bepaald worden of de partij geautoriseerd is.

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 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.

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