



Evaluatierapport

SBR Vernieuwing

Lars Mosterd, 18 juli 2022

Versie: 1.0

Inhoudsopgave

Inhoudsopgave	2
Introductie	3
Hoe draagt TIP bij aan SBR. Een onderzoek middels vijf experimenten	4
Experiment 1 End-to-end demo	7
Experiment 2 Standaard uitwisselen	8
Experiment 3 Machtigen	10
Experiment 4 Gebruik toegevoegde waarde dienst	13
Experiment 5 Delen gekwalificeerde subset	16
3 Overkoepelende resultaten	19
4 Conclusies	19
5 Vervolgstappen	21
6 Relatie tot andere activiteiten	21
Appendix A: Knelpunten uit business analyse	22

Introductie

Met een business analyse en een serie experimenten is onderzocht wat de toegevoegde waarde van het Trusted Information Partners (TIP¹) initiatief is voor SBR. Dit evaluatierapport is een reflectie op de onderzoeksvraag en de doelstellingen zoals opgesteld in het plan van aanpak² en de uitgevoerde experimenten. Op basis van de uitgevoerde experimenten zijn conclusies getrokken en vervolgstappen gedefinieerd. Ook is in dit rapport de relatie beschreven tussen activiteiten van SBR, TIP en de Belastingdienst.

¹ Binnen TIP onderzoeken publieke en private partijen hoe een domeinoverstijgend ecosysteem voor eenvoudige en betrouwbare informatie-uitwisseling eruit kan zien. Voor meer context zie: TIP. 03-2022. *Two-pager: Eenvoudig en betrouwbaar online zakendoen.*

² SBR Vernieuwing. 23-06-2020. *Beproeven Trusted Online Ecosysteem in het kader van SBR Vernieuwing.*

Hoe draagt TIP bij aan SBR.

Een onderzoek middels vijf experimenten

Dit evaluatierapport gaat uit van de onderzoeksvraag zoals geformuleerd in het plan van aanpak:

Hoe kan het Trusted Online Ecosysteem (of TIP-ecosysteem), gebaseerd op eIDAS vertrouwensdiensten, bijdragen aan het SBR afsprakenstelsel?

Het theoretische antwoord op deze vraag is geformuleerd in de business analyse “toepassing van een Trusted Online Ecosysteem voor SBR”³, waarin de de IB-keten van de Belastingdienst is gebruikt als representatieve use case. De conclusies betreffende deze use case zijn samengevat in Appendix A.

Naar het praktische antwoord is gezocht middels vijf experimenten. Het overkoepelende doel van de experimenten is tweeledig:

1. theoretische conclusies uit de business analyse onderbouwen door de gekozen oplossingsrichting te toetsen met experimenten;
2. creëren van draagvlak voor de gekozen oplossingsrichting.

De experimenten richten zich op de volgende specifieke doelstellingen uit het plan van aanpak:

1. Vaststellen technologische toepasbaarheid:
 - a. Betrokken actoren zijn te authenticeren op een hoog betrouwbaarheidsniveau.
 - b. Betrokken actoren hebben tijdens de gegevensuitwisseling inzicht in de status van het proces.
 - c. Vertegenwoordiging door een intermediair en instemming van de belanghebbende kan worden bewezen met onweerlegbare vastlegging van wilsuiting en toestemming.
 - d. Er kan op een veilige manier gebruik gemaakt worden van informatiediensten (red: cq. toegevoegde waarde diensten) van vertrouwde derde partijen. Informatiediensten kunnen aangesproken worden om o.a.:

³ SBR Vernieuwing. 04-05-2020. *Business analyse: toepassing van een Trusted Online Ecosysteem voor SBR.*

- i. De authenticiteit van uitgewisselde gegevens te verifiëren;
 - ii. De datakwaliteit van uitgewisselde gegevens te controleren;
 - e. Gegevens zijn herbruikbaar over domeinen.
2. Vaststellen van interoperabiliteit van de benodigde standaarden met bestaande standaarden.

Er zijn vijf experimenten uitgevoerd. Doel van de eerste vier experimenten is om aan te tonen dat TIP invulling kan geven aan belangrijke SBR bouwblokken en dat TIP een aantal knelpunten in de huidige implementatie van SBR oplost. Het vijfde experiment heeft als doel om te laten zien wat de mogelijkheden zijn van een open en domeinoverstijgend ecosysteem. In het vervolg van dit hoofdstuk komt elk van de experimenten in detail aan de orde. Een overzicht van de verschillende experimenten vindt u op de volgende pagina.

5 experimenten

die de meerwaarde van TIP voor SBR tonen

1

End-to-end demo

Met behulp van een gesimuleerde front-end wordt de gehele IB-keten in de gewenste situatie getoond vanuit het perspectief van de belanghebbende en intermediair. **Geeft inzicht in de werking van TIP.**

2

Standaard uitwisselen

Een belanghebbende vraagt zijn VIA-gegevens op bij de Belastingdienst. **Toont de werking en toepasselijkheid van de basisfunctie 'Veilig uitwisselen' aan.**

3

Machtigen

Een belanghebbende machtigt zijn intermediair zodat deze zijn VIA-gegevens kan ophalen bij de Belastingdienst. **Toont de werking en toepasselijkheid van de basisfunctie 'Machtigen' aan.**

4

Gebruik toegevoegde waarde dienst

Een belanghebbende gebruikt een toegevoegde waarde dienst om zijn aangifte inkomstenbelasting te valideren op XBRL validiteit alvorens deze in te dienen bij de Belastingdienst. **Toont hoe toegevoegde waarde diensten van derden ontsloten kunnen worden binnen TIP en laat zien hoe deze kunnen worden toegepast in de context van SBR.**

5

Delen gekwalificeerde subset

In dit experiment deelt een consument een gedeelte van zijn VIA-gegevens met ING Real Estate Finance (REF) als input voor een kredietwaardigheidstoets. **Laat zien wat de toegevoegde waarde is van een domeinoverstijgend ecosysteem.**

Experiment 1 | End-to-end demo

Beschrijving

In het eerste experiment wordt, met een demo, de gehele IB-keten in de gewenste situatie getoond vanuit het perspectief van de eindgebruiker (belanghebbende en intermediair). De interacties die een gebruiker heeft met ketenpartijen en toegevoegde waarde diensten zijn gesimuleerd. Voor de gebruiker zijn de handelingen en terugkoppelingen vergelijkbaar met die in een functionerend ecosysteem. De demo maakt ook inzichtelijk wat er ‘onder de motorkap’ gebeurt en welke zekerheden dat geeft voor belanghebbende, intermediair en Belastingdienst.

Doelstelling

Doel van deze demo is om de gewenste eindsituatie inzichtelijk en tastbaar te maken. Het maakt visueel en interactief (clickable) duidelijk hoe het ecosysteem voor gebruikers werkt en wat de voor- en nadelen zijn. De demo is daarmee ook een communicatie-instrument waarmee draagvlak gevormd kan worden voor vervolg experimenten.

Resultaten

De demo is positief ontvangen binnen SBR Vernieuwing en de Belastingdienst. Door de demo is meer inzicht ontstaan in de gewenste situatie en zijn vervolg experimenten aangescherpt. De demo is gebruikt om bij diverse partijen binnen TIP, hun achterban en externe partners, duidelijker te maken waar TIP over gaat.

Conclusie

Mede dankzij de demo is er voldoende draagvlak bij SBR Vernieuwing en de Belastingdienst om verder te gaan met de overige experimenten.

Experiment 2 | Standaard uitwisselen

Beschrijving

In dit experiment vraagt een belanghebbende op basis van zijn identificerend nummer (BSN) vanuit zijn handelingsomgeving de gegevens van een Vooraf Ingevulde Aangifte (VIA) op bij de Belastingdienst. De belanghebbende handelt uitsluitend voor zichzelf door zelf zijn VIA-gegevens op te vragen en te ontvangen. De systemen van de Belastingdienst worden gesimuleerd middels een smart stub en er wordt gebruik gemaakt van fictieve identiteiten/identificerende nummers. De smart stub van de Belastingdienst heeft een vaste delegatieregeling, waarbij vastgesteld is dat een verzoek voor de belanghebbende ingewilligd kan worden als dit dezelfde persoon is als waar de opgevraagde VIA betrekking op heeft. De functionaliteit voor *Veilig uitwisselen* wordt ingericht met de gekwalificeerde eIDAS vertrouwensdienst voor *Elektronische Aangetekende Bezorging* (i.e. qERDS). In het experiment wordt gebruik gemaakt van één qERDS-provider.

Doelstelling

Doel van het experiment is aantonen dat de SBR functionaliteiten voor het veilig uitwisselen van informatie kunnen worden ingericht met gekwalificeerde eIDAS vertrouwensdiensten en de principes van TIP. Een succesvol experiment toont in essentie de werking en toepasbaarheid van de basisfunctionaliteit *Veilig uitwisselen* voor SBR aan. Daarnaast richt dit experiment zich op het aantonen van de volgende specifieke doelstellingen, die zijn geformuleerd op basis van de knelpunten beschreven in Appendix A.

- Vaststellen technologische toepasbaarheid op de volgende facetten:
 - betrokken actoren zijn te authenticeren op een hoog betrouwbaarheidsniveau;
 - actoren hebben (verbeterd) inzicht in de status van het gegevensuitwisselingsproces.
- Vaststellen interoperabiliteit van de benodigde en bestaande standaarden.

Resultaten

Naast een werkende experiment-omgeving leidde dit experiment tot een eerste set aan specificaties voor de inrichting van de basisfunctionaliteit *Veilig Uitwisselen*. Daarmee is het hierboven genoemde doel bereikt. De betrokken partijen hebben aangegeven graag mee te willen werken aan de vervolgstappen om te komen tot een grootschalige toepassing op productie, waaronder het nader specificeren van de standaard.

Ten aanzien van de specificaties:

- De eIDAS vertrouwensdienst voor berichtuitwisseling – gekwalificeerde elektronische aangetekende bezorging (qERDS – Qualified Electronic Registered Delivery Service) – is gebruikt voor het uitwisselen van de VIA-Gegevens en het verzoek daartoe.
- Er is gebruik gemaakt van gekwalificeerde elektronische handtekeningen en seals om de authenticiteit van de uitgewisselde berichten te garanderen.
- De Belastingdienst verkrijgt zekerheid over het BSN van de belanghebbende op basis van een SAML-assertion die is geseald door de QTSP.

Conclusies

Met de technische validatie door architecten van de betrokken partijen (SBR Vernieuwing, Digicampus, de Belastingdienst, Cleverbase, Visma, NVM, HDN en ING), zijn de volgende conclusies over het experiment en de opgestelde specificaties geformuleerd:

- De gevalideerde standaarden vormen een goede basis voor system-to-system informatie-uitwisseling binnen TIP. Het internationale en open karakter van de standaarden waarop is voortgebouwd, is hiervoor aangedragen als belangrijke reden.
- Het is van belang dat de aangesloten partijen betrokken blijven bij de nadere specificering van de standaard en dat deze open beschikbaar wordt gemaakt. Cleverbase heeft aangegeven hier invulling aan te willen geven door het project onder te brengen in een open source community.
- Om een stelsel met meerdere aanbieders van ERDS's mogelijk te maken wordt in de nadere specificatie toegewerkt naar een four corner model zoals benoemd in ETSI EN 319 522.

Een openstaande vraag die moet worden opgelost in het procesontwerp is hoe om te gaan met identificerende nummers. Momenteel verstrekt de Belastingdienst gegevens op basis van een BSN-nummer. Zonder grondslag mag een private partij (zoals een vertrouwensdienstverlener) echter geen BSN verwerken.

Experiment 3 | Machtigen

Beschrijving

In dit experiment machtigt een belanghebbende zijn intermediair zodat deze zijn VIA-gegevens kan ophalen. Het gaat nog steeds om fictieve entiteiten. De smart stub van de Belastingdienst heeft een aanvullende delegatieregeling, waarbij vastgesteld is dat een verzoek ingewilligd kan worden als dit dezelfde persoon is als waar de opgevraagde VIA betrekking op heeft of als er een verzoek komt van een actor die beschikt over een geldige machtigingsverklaring.

Ten aanzien van machtigen zijn er in de soll-situatie meerdere oplossingsrichtingen mogelijk. In dit experiment is voor een eenvoudig te implementeren oplossing gekozen om de werkingsprincipes van het ecosysteem laagdrempelig te kunnen testen (ondertekening van een machtigingsclaim die niet centraal verifieerbaar wordt vastgelegd maar wordt meegestuurd als de derde partij namens de belanghebbende handelt). Het valt nadrukkelijk buiten scope van de experimenten om een machtigingsarchitectuur te ontwerpen voor een going concern situatie.

Doelstelling

Doel van het experiment is aantonen dat de SBR functionaliteiten voor machtigen kunnen worden ingericht met gekwalificeerde eIDAS vertrouwensdiensten en de principes van TIP. Een succesvol experiment toont in essentie de werking en toepasbaarheid van de basisfunctionaliteit *Machtigen* voor SBR aan. Daarnaast richt dit experiment zich op het aantonen van de volgende specifieke doelstellingen, die zijn geformuleerd op basis van de geïdentificeerde knelpunten zoals beschreven in Appendix A.

- Vaststellen technologische toepasselbaarheid op de volgende facetten:
 - betrokken actoren hebben tijdens de gegevensuitwisseling (meer) inzicht in de status van het proces;
 - vertegenwoordiging en instemming van belanghebbende door een intermediair kan worden geëxpliciteerd door onweerlegbare vastlegging van wilsuiking en toestemming;

Resultaten

Naast een werkende experimentomgeving leidt dit experiment ook tot een eerste set specificaties voor de inrichting van de basisfunctionaliteit *Machtigen* binnen TIP. In dit experiment is het machtigingsvraagstuk benaderd vanuit een Self Sovereign Identity (SSI) paradigma, wat inhoudt dat de belanghebbende degene is die de machtigingsverklaring

verstrekt in plaats van een machtigingenregister (Identity Federation paradigma). Toch is de gekozen oplossing vrij eenvoudig te vertalen naar een situatie met een machtigingenregister.

Ten aanzien van de specificaties:

- De eIDAS vertrouwensdienst voor berichtuitwisseling – gekwalificeerde elektronische aangetekende bezorging (qERDS – Qualified Electronic Registered Delivery Service) – is gebruikt voor het uitwisselen van de machtigingsverklaring en het verzoek daartoe.
- Er is gebruik gemaakt van gekwalificeerde elektronische handtekeningen en seals om de authenticiteit van de uitgewisselde berichten te garanderen.
- Voor het opstellen van de machtigingsverklaring en het verzoek daartoe is gebruik gemaakt van XACML. De keuze voor deze standaard moet verder worden onderzocht.

Conclusies

Architecten van de betrokken partijen (SBR Vernieuwing, Digicampus, de Belastingdienst, Cleverbase, Visma, NVM, HDN en ING) trekken gezamenlijk onderstaande conclusies over het experiment en de opgestelde specificaties. Ook zijn een aantal concrete vervolgstappen benoemd.

Het lijkt technisch goed mogelijk om via een qERDS...

- ... een verzoek tot informatie van actor A te voorzien van een door actor B gekwalificeerd ondertekende/gesealde autorisatietoekenning. Zodat de informatie verstrekkende actor C met een hoog betrouwbaarheidsniveau, op basis van een bestaand autorisatiebeleid, geautomatiseerd kan vaststellen of de informatie aan de verzoekende actor A verstrekt kan worden;
- ... actor A een verzoek te laten doen aan actor B voor het tekenen van een autorisatietoekenning, waarop actor B dit verzoek kan inwilligen door een autorisatietoekenning te ondertekenen/sealen en deze via de qERDS aan actor A te verstrekken.

Dit betekent dat de qERDS standaarden voor berichtuitwisseling de functionaliteit voor machtigen in het ecosysteem kunnen faciliteren mits deze ook geschikt zijn voor toepassing op grote schaal, in een context waar robuustheid belangrijk is. In het TIP platform overleg is vastgesteld dat er op het niveau van TIP (en dus niet op domeinniveau) gestandaardiseerd dient te worden rondom de functionaliteit voor machtigen.

Bij het nader specificeren van de functionaliteit voor machtigen moet de juridische context goed in ogenschouw worden genomen. Oplossingen voor machtigen ontstaan vaak vanuit de beschikbare technische protocollen. Om tot een schaalbare oplossing te komen is het noodzakelijk om eerst de juridische vereisten uiteen te zetten. De volgende onderwerpen moeten in een memo worden uitgewerkt zodat deze besproken kunnen worden in de technische werkgroep: (1) schaalbaarheid qERDS, (2) keuze voor XACML, (3) onderscheid tussen volmacht en autorisatie, (4) eisen aan signature applications, (5) gebruik van BSN voor identificatie belanghebbende

Experiment 4 | Gebruik toegevoegde waarde dienst

Beschrijving

In dit experiment gebruikt een belanghebbende een toegevoegde waarde dienst om zijn aangifte inkomstenbelasting te valideren op XBRL-validiteit alvorens deze in te dienen bij de Belastingdienst. Het oordeel van de toegevoegde waarde dienst wordt vastgelegd op een manier die inzichtelijk is voor de Belastingdienst (of andere ketenpartijen) en maakt het mogelijk om de authenticiteit van het oordeel vast te stellen. Het oordeel is onlosmakelijk verbonden aan het gevalideerde bericht. Omdat in dit experiment met name gebruik wordt gemaakt van functionaliteit die in experiment 2 (standaard uitwisselen) is beproefd, ligt de focus op de conceptuele uitwerking van de manier waarop toegevoegde waarde diensten van derde partijen ontsloten kunnen worden binnen TIP.

Doelstelling

Doel van het experiment is aantonen dat de SBR functionaliteiten voor berichtvalidatie kunnen worden ingericht met gekwalificeerde eIDAS vertrouwensdiensten en de principes van TIP. Een succesvol experiment toont aan hoe toegevoegde waarde diensten van derden ontsloten kunnen worden binnen TIP en laat zien hoe deze kunnen worden toegepast in de context van SBR. Daarnaast richt dit experiment zich op het aantonen van de volgende specifieke doelstelling, die is geformuleerd op basis van de geïdentificeerde knelpunten zoals beschreven in Appendix A.

- Vaststellen technologische toepasselijkheid op het volgende facet:
 - er kan op een veilige manier gebruik gemaakt worden van informatiediensten (red: cq. toegevoegde waarde diensten) van vertrouwde derde partijen. Informatiediensten (red: cq. toegevoegde waarde diensten) kunnen aangesproken worden om o.a.:
 - de datakwaliteit van uitgewisselde gegevens te controleren.

Resultaten

Het experiment heeft geleid tot een eerste gevalideerde set aan specificaties voor het gebruik van toegevoegde waarde diensten binnen TIP. De oplossing is aan een brede groep stakeholder getoond in een demo.

Het uitgangspunt en centrale idee in de specificaties is dat ketenspecificaties (w.o. de aanleverspecificaties) worden gepubliceerd in de vorm van signature policies. Daarmee kan het waardeoordeel van de toegevoegde waarde dienst de vorm krijgen van een gekwalificeerde

elektronische handtekening waarin wordt verwezen naar de signature policy en het specifieke commitment type dat binnen de signature policy is gedefinieerd en dat specificeert welke validatie is uitgevoerd.

Doordat het waardeoordeel de vorm heeft van een detached signature is het mogelijk om in een later stadium meerdere waardeoordelen die betrekking hebben op één bestand te 'stapelen'. In het geval van een aangifte die wordt aangeleverd bij de Belastingdienst zou dit bijvoorbeeld kunnen betekenen dat naast het waardeoordeel van de XBRL-validator, ook een verklaring van de intermediair wordt toegevoegd dat deze heeft gehandeld in overeenstemming met de vereisten van Horizontaal Toezicht.

Ten aanzien van de specificaties.

- De eIDAS vertrouwensdienst voor berichtuitwisseling – gekwalificeerde elektronische aangetekende bezorging (qERDS – Qualified Electronic Registered Delivery Service) – is gebruikt voor de uitwisseling van de berichten tussen de Belastingdienst, de belanghebbende en de leverancier van de toegevoegde waarde dienst.
- Er is gebruik gemaakt van gekwalificeerde elektronische handtekeningen en seals om de authenticiteit van de uitgewisselde berichten te garanderen.
- De ketenspecificaties zijn opgesteld in de vorm van een signature policy conform ETSI TS 119 172-1 en ETSI TS 119 172-2.
- Het waardeoordeel van de informatiedienst heeft de vorm van een *detached* gekwalificeerde elektronische handtekening⁴ met een expliciete verwijzing naar:
 - de signature policy die tevens de ketenspecificaties bevat;
 - een commitment type (gespecificeerd in de signature policy) dat het inhoudelijke waardeoordeel bevat;
 - de data waar het waardeoordeel betrekking op heeft;
- De vraag-antwoord berichten voor de opdrachtverstrekking aan de toegevoegde waarde dienst en de response daarop, zijn opgesteld in XML op basis van een zelf gedefinieerde standaard voor een *DocumentClaim* verzoek binnen TIP.
 - In het verzoek wordt verwezen naar:
 - het gevraagde waardeoordeel middels een verwijzing naar bovengenoemd commitment type en signature policy;

⁴ N.B. in deze specifieke use case betrof het een XAdES B-B handtekening conform ETSI 319 132-1.

- het document waar het gevraagde waardeoordeel betrekking op moet hebben middels een hash.
- In de response wordt verwezen naar het waardeoordeel (detached signature) middels een hash.

Conclusies

Architecten van de betrokken partijen (SBR Vernieuwing, Digicampus, de Belastingdienst, Cleverbase, Visma, NVM, HDN en ING) trekken gezamenlijk onderstaande conclusies over het experiment en de opgestelde specificaties:

- Het lijkt technisch goed mogelijk om, gebruikmakend van een qERDS, een databestand van actor A te voorzien van een door actor B gekwalificeerd ondertekende/ gesealde kwaliteitsclaim. zodat de uitvragende actor C met een hoog betrouwbaarheidsniveau, op basis van een bestaand beleid, geautomatiseerd vast kan stellen of de aangeleverde informatie voldoet aan de gewenste kwaliteit.
- Het lijkt technisch goed mogelijk om met een qERDS Actor A een verzoek tot het afgeven van een datakwaliteitsclaim te laten doen aan actor B, waarop actor B dit verzoek (geautomatiseerd) kan inwilligen door de claim via de qERDS aan actor A te verstrekken.
- Signature policies maken het mogelijk om op een efficiënte en gestandaardiseerde manier ketenspecificaties vast te leggen. Daarmee kan de bovengenoemde datakwaliteitsclaim de vorm krijgen van een detached signature waarin verwezen wordt naar een commitmenttype dat gespecificeerd is in de signature policy waarin de ketenspecificaties zijn vastgelegd.

Experiment 5 | Delen gekwalificeerde subset

Beschrijving

In dit experiment deelt een consument een gedeelte van zijn VIA-gegevens met ING Real Estate Finance (REF), als input voor een kredietwaardigheidstoets. In lijn met het data-minimalisatie principe uit de AVG is het belangrijk dat enkel die gegevens worden gedeeld die noodzakelijk zijn voor het beoogde doel. Daarnaast is het van belang dat ING REF erop kan vertrouwen dat:

- de aangeleverde subset van de VIA-gegevens haar oorsprong vindt in de VIA-gegevens die zijn verstrekt door de Belastingdienst;
- de subset gecreëerd is conform de specificaties die de ING heeft opgesteld.

De subset is gecreëerd door de handelingsomgeving van de belanghebbende zodat bovengenoemde zekerheden ontleent kunnen worden aan een verklaring van een vertrouwde derde partij; in dit geval een QTSP. Omdat in dit experiment met name gebruik is gemaakt van functionaliteit die in experiment 2 (standaard uitwisselen) is beproefd, ligt de focus binnen dit experiment op de conceptuele uitwerking van de manier waarop interactie plaatsvindt tussen actoren uit verschillende domeinen.

Doelstelling

Dit experiment richt zich op het delen van gegevens tussen actoren afkomstig uit verschillende domeinen. Doel van het experiment is om de toegevoegde waarde van een domeinoverstijgend ecosysteem aan te tonen. Specifiek laat dit experiment zien dat data heel gericht gedeeld kunnen worden door het afschermen van gevoelige persoonsgegevens, die de ontvangende partij niet nodig heeft of geen recht op heeft, terwijl de authenticiteit van de brondata wel kan worden vastgesteld. Het experiment richt zich daarmee op de volgende specifieke doelstelling, die is geformuleerd op basis van de geïdentificeerde knelpunten zoals beschreven in Appendix A.

- Vaststellen technologische toepasselijkheid op het volgende facet:
 - gegevens zijn herbruikbaar over domeinen.

Resultaten

Het experiment heeft geleid tot een succesvolle demo waarin is aangetoond dat bestaande technologie gebruikt kan worden om een “gekwalificeerde subset” te creëren en te delen over domeinen heen, inclusief eerste aanzet tot specificaties op gebied van gegevens, processen & techniek. Deze uitwerking en specificaties zijn in lijn met de uitgangspunten van TIP en bouwen

voort op de voorgaande experimenten. Hiermee wordt de toepasbaarheid van eerder gevalideerde concepten in een nieuwe use case aangetoond.

Bij de uitwerking van het experiment en de demo zijn meerdere partijen betrokken geweest (SBR Vernieuwing, Belastingdienst, Cleverbase, Visma Connect, ING). De uitwerking is gevalideerd binnen de werkgroep Techniek van TIP, waarin alle deelnemende partijen zijn vertegenwoordigd. Daarnaast heeft dit experiment geleid tot een vergroting van de bekendheid en het draagvlak voor TIP, wat blijkt uit de toenemende interesse voor de demo en de positieve reacties achteraf.

Ten aanzien van de specificaties:

- De eIDAS vertrouwensdienst voor berichtuitwisseling – gekwalificeerde elektronische aangetekende bezorging (qERDS – Qualified Electronic Registered Delivery Service) – is gebruikt voor de uitwisseling van de berichten tussen de Belastingdienst, de belanghebbende en ING.
- Er is gebruik gemaakt van gekwalificeerde elektronische handtekeningen en seals om de authenticiteit van de uitgewisselde berichten te garanderen.
- De ketenspecificaties zijn opgesteld in de vorm van een signature policy conform ETSI TS 119 172-1 en ETSI TS 119 172-2. In dit experiment is zijn de signature policies modulair opgezet middels een hiërarchie gebaseerd op de *North American Industry Classification Standard (NAICS)*.
- Om de authenticiteit van de subset te borgen en om te verklaren dat deze is opgesteld conform de specificaties van de ING, geeft de QTSP die de subset opstelt en verstrekt een waardeoordeel af die de vorm heeft van een *detached* gekwalificeerde elektronische handtekening. Dit is op dezelfde manier gedaan als in experiment 4. Hiermee wordt de toepasbaarheid van de daar gehanteerde standaarden in een nieuwe use case aangetoond.
- De vraag-antwoord berichten voor het verzoek om de gekwalificeerde subset en de response daarop, zijn opgesteld in XML.
 - De vraag-antwoord berichten voor het waardeoordeel maken gebruik van dezelfde standaard als gedefinieerd in experiment 4 (i.e. *DocumentClaim*).
 - De vraag-antwoord berichten voor de subset zelf maken gebruik van een vergelijkbare standaard die is gedefinieerd in de context van dit experiment (i.e. *DocumentRequest*).

Conclusies

Dit experiment laat zien wat de mogelijkheden zijn van een open en domeinoverstijgend ecosysteem, waar SBR onderdeel van is. Aangetoond is dat TIP technisch geschikt is om gegevens domeinoverstijgend te hergebruiken. Architecten van de betrokken partijen (SBR Vernieuwing, Digicampus, de Belastingdienst, Cleverbase, Visma, NVM, HDN en ING) hebben gezamenlijk onderstaande conclusies getrokken over het experiment en de opgestelde specificaties:

- Het is technisch goed mogelijk om een subset te maken van een databestand, op basis van eerder gepubliceerde specificaties, waarbij de relying party erop kan vertrouwen dat de gegevens in de betreffende subset afkomstig zijn uit het originele bestand en dat de subset is gecreëerd conform de gepubliceerde specificaties.
- Het is technisch goed mogelijk om, gebruikmakend van een qERDS, een databestand van actor A te voorzien van een door actor B gekwalificeerd ondertekende/ gesealde kwaliteitsclaim zodat de uitvragende actor C met een hoog betrouwbaarheidsniveau, op basis van een bestaand beleid, geautomatiseerd vast kan stellen of de aangeleverde informatie voldoet aan de gewenste kwaliteit (ook geconcludeerd n.a.v. exp #4).
- Het is technisch goed mogelijk om met een qERDS actor C een verzoek tot het afgeven van een (1) dataset, en (2) een datakwaliteitsclaim over de afgegeven dataset te laten doen aan actor A, waarop actor A dit verzoek gemakkelijk kan inwilligen door de dataset en claim (geautomatiseerd) te verkrijgen van actor B.
- Signature policies maken het mogelijk om op een efficiënte en gestandaardiseerde manier ketenspecificaties vast te leggen (ook geconcludeerd n.a.v. exp #4)

3 Overkoepelende resultaten

Door de resultaten van de verschillende experimenten te combineren, komen we tot de volgende overkoepelende resultaten:

- Meer inzicht in de gewenste Soll-situatie. Mede op basis hiervan kan de werkgroep Techniek van TIP binnen drie maanden een globale technische architectuur van het ecosysteem ontwerpen. Deze globale technische architectuur kan de basis zijn voor een verdere uitwerking van de basisfunctionaliteiten tot concrete specificaties (zie ook *Vervolgstappen*).
- Gevalideerde⁵ set aan specificaties die een goede basis vormen voor de invulling van een aantal belangrijke basisfunctionaliteiten: *Ondertekenen, Veilig uitwisselen, Machtigen, Toegevoegde waarde diensten gebruiken*. Op basis van de uiteindelijke specificaties kunnen softwareleveranciers producten leveren die compatibel zijn met TIP.
- Vijf drukbezochte (50+ deelnemers) en goed gewaardeerde demo's die hebben geleid tot een vergroot draagvlak voor TIP bij relevante stakeholders (zie *Conclusies*).
- Concrete aanknopingspunten om de verbinding tussen TIP en andere relevante initiatieven te leggen, waaronder Zorgeloos Vastgoed en SBR Assurance.

4 Conclusies

Zoals genoemd in de inleiding was de doelstelling van de experimenten tweeledig:

1. het bewijzen van de theoretische conclusie uit de business analyse dat TIP van toegevoegde waarde is voor SBR;
2. creëren van draagvlak voor een domeinoverstijgend, open ecosysteem gebaseerd op gekwalificeerde vertrouwensdiensten (cq. TIP).

⁵ De resultaten van elk experiment zijn in een technische validatiesessie met architecten van de betrokken partijen gevalideerd.

Wat betreft de eerste doelstelling wordt, op basis van de uitgevoerde experimenten, geconcludeerd dat TIP invulling kan geven aan de belangrijkste SBR bouwblokken en dat TIP een aantal knelpunten in de huidige implementatie van SBR oplost (zie ook Appendix A).

- Door de belanghebbende te laten instemmen met een machtigingsverzoek middels een gekwalificeerde elektronische handtekening, kan het machtigingsproces volledig digitaal, en daarmee efficiënter en veiliger, worden ingericht.
- Door de belanghebbende de aangifte te laten ondertekenen met een gekwalificeerde elektronische handtekening voordat deze wordt ingediend bij de Belastingdienst kan de belanghebbende expliciet toestemming geven voor het indienen van zijn/haar aangifte en verklaren in te stemmen met de inhoud daarvan.
- TIP maakt het voor alle betrokken partijen mogelijk om op een toegankelijke manier, met een hoge mate van betrouwbaarheid online zaken te doen. Hierdoor kunnen de betrokken partijen hetzelfde 'kanaal' gebruiken en komt de belanghebbende centraal te staan in de informatie-uitwisseling. Dit houdt in dat zij via één kanaal alle correspondentie mbt de IB-keten kan ontvangen en rechtstreekse terugkoppeling kan krijgen van de intermediair en/of de Belastingdienst. Dit draagt bij aan een sterke regiepositie voor de belanghebbende.
- Doordat alle betrokken partijen gebruik maken van gekwalificeerde certificaten kan onweerlegbare identificatie plaatsvinden op actor-niveau zodat de Belastingdienst en andere ketenpartijen met meer zekerheid kunnen vaststellen wie betrokken is bij de informatie-uitwisseling.

Het vijfde experiment laat zien dat het van toegevoegde waarde is om, als SBR, aan te sluiten op een ecosysteem waarbinnen informatie wordt uitgewisseld tussen een groot aantal domeinen omdat daarmee de herbruikbaarheid van gegevens wordt vergroot. Hoewel SBR ook een domeinoverstijgend afsprakenstelsel is, beoogd TIP een afsprakenstelsel te zijn dat van toepassing is op een nog veel groter aantal domeinen.

Ook de tweede doelstelling is bereikt; de experimenten hebben bijgedragen aan het creëren van draagvlak voor een domeinoverstijgend, open ecosysteem gebaseerd op gekwalificeerde vertrouwensdiensten. De experimenten en demo's hebben tot meer bewustwording geleid bij verschillende partijen; zowel binnen als buiten de Belastingdienst en SBR. Daarnaast hebben de resultaten geleid tot een aantal concrete aanknopingspunten om met relevante partijen in gesprek te gaan en hen te betrekken bij TIP.

5 Vervolgstappen

Op basis van de uitgevoerde experimenten worden onderstaande vervolgstappen voorgesteld:

- Uitwerken van een globale technische architectuur van TIP op basis van de resultaten van deze experimentenreeks, de *Willeke paper*⁶ en de *Greenpaper*⁷. Deze technische architectuur beschrijft de basisfunctionaliteiten, de manier waarop deze ingevuld worden en hoe ze zich tot elkaar verhouden. Deze uitwerking biedt voldoende kaders om de losse basisfuncties verder uit te werken tot een set aan specificaties voor architecten met relevante domeinkennis.
- Inrichten van een efficiënte TIP governance die innovatie én standaardisatie stimuleert, recht doet aan specifieke kenmerken en eisen van domeinen maar ook domeinoverstijgend handelen mogelijk maakt.
- Verder uitwerken, bouwen en implementeren! Hierbij is het belangrijk rekening te houden met de veranderopgave (legacy software én kennis) van de verschillende organisaties. De eerste stap is mensen en organisaties de middelen geven die het mogelijk maken op een eenvoudige en betrouwbare manier digitaal zaken te doen. Dit zijn in de eerste plaats gekwalificeerde certificaten (zoals bedoeld in eIDAS) en de mogelijkheid om deze te gebruiken.

6 Relatie tot andere activiteiten

De technische uitwerking van de globale architectuur, basisfuncties en de opgeworpen punten in de technische evaluatie sessies worden geprioriteerd en uitgevoerd in de werkgroep Techniek van TIP. De governance van TIP wordt verder uitgewerkt binnen de werkgroep Governance van TIP.

De toepassing van de architectuur wordt geprioriteerd en uitgevoerd binnen de Keten Interactie van de Belastingdienst, in afstemming met externe partners als softwareleveranciers en fiscaal dienstverleners.

Het opnemen van (elementen van) het TIP Afsprakenstelsel in het SBR Afsprakenstelsel wordt geprioriteerd en uitgevoerd in de SBR Expertgroep Gegevens, Processen en Techniek.

⁶ Dijkhuis, S., Van Wijk, R., Dorhout, H., & Bharosa, N., 2018, When Willeke can get rid of paperwork: A lean infrastructure for qualified information exchange based on trusted identities. Zie link.

⁷ Van Wijk, R., Van Oosterhout, R., Klimbie, R., Mulder, M., 24-10-2019, Greenpaper: Vertrouwd S2S Ecosysteem. Op aanvraag beschikbaar.

Appendix A: Knelpunten uit business analyse

Tabel 1: overzicht knelpunten in huidige inrichting IB-keten

Knelpunt	Oorzaak	Probleem	Gevolg
1. Modaliteiten van machtigingen-proces	De belanghebbende kan zijn intermediair niet digitaal machtigen	De belanghebbende kan zijn intermediair enkel machtigen via een proces dat gedeeltelijk via de post verloopt	Dit proces geeft beperkte zekerheid, is duur en heeft een coördinatie last.
2. Impliciete vertegenwoordiging voor aanleveren aangifte	De belanghebbende kan niet online handelen ⁸ met voldoende rechtszekerheid.	De belanghebbende geeft geen expliciete toestemming voor het indienen van de aanslag	Indien er een geschil ontstaat moet eerst worden gereconstrueerd wat er exact is gebeurd in de relatie tussen de belanghebbende en de intermediair.
3. Ongestructureerde communicatie tussen belanghebbende en intermediair	Het proces verloopt vanuit het perspectief van de belanghebbende over tijd via verschillende kanalen	Communicatie tussen de intermediair en de belanghebbende is veelal ongestructureerd.	Hogere administratieve last en grotere kans op fouten in de dataverwerking.
4a. Geen transparant procesverloop voor belanghebbende		Onoverzichtelijk procesverloop	Dit proces zorgt voor onzekerheid en is tijdrovend (voor zowel de belanghebbende als intermediair)
4b.		Belanghebbende en Belastingdienst kunnen niet rechtstreeks digitaal communiceren	Interacties vinden enkel plaats tussen de intermediair en de Belastingdienst. De belanghebbende krijgt geen rechtstreekse terugkoppeling over het indienen van de Aangifte IB en het voldoen aan zijn aangifteplicht.
4c.		De belanghebbende heeft geen	Onzekerheid voor

⁸ Om online te kunnen handelen met voldoende rechtszekerheid moet de belanghebbende zich met hoge mate van zekerheid kunnen authenticeren, stukken kunnen ondertekenen en informatie op een veilige en betrouwbare manier kunnen uitwisselen.

		inzicht in zijn actieve machtigingsregistraties en krijgt ook geen terugkoppelingen over wijzigingen van de registraties (activering en intrekking).	belanghebbende en hoge kosten in het geval van een geschil.
5. Beperkt hergebruik van data	Wederpartijen beschikken vaak niet over technisch interoperabele kanalen en de belanghebbende heeft zelf niet de beschikking heeft over zijn data.	Het is voor de belanghebbende lastig om data die op hem betrekking heeft (zoals de VIA, de SBA, maar ook de aangifte) te delen met andere partijen.	Dubbel werk en administratieve last voor de belanghebbende
6. Identificatie niet op actor-niveau	Gebrek aan breed beschikbaar hebben van persoonsgebonden en organisatiegebonden PKIoverheid certificaten.	Identificatie vindt plaats op basis van PKIoverheid servercertificaten.	De belastingdienst weet niet met welke actor er informatie wordt uitgewisseld.

Tabel 2: implicaties gekozen oplossingsrichting voor geïdentificeerde knelpunten

Knelpunt	Oplossing in Soll-situatie	Resultaat
1. Modaliteiten van machtigingen-proces	Belanghebbende geeft instemming op machtigingsverzoek intermediair met gekwalificeerde elektronische handtekening.	Machtigingsrelatie intermediair - belanghebbende digitaal verifieerbaar door direct mee verzonden expliciete consent.
2. Impliciete vertegenwoordiging voor aanleveren aangifte	Belanghebbende ondertekend aangifte met gekwalificeerde elektronische handtekening voor indiening door intermediair	Vertegenwoordiging expliciet en onweerlegbaar vastgelegd in aangifte
3. Ongestructureerde communicatie tussen belanghebbende en intermediair	Belanghebbende ontvangt via één kanaal alle correspondentie mbt de IB-keten en krijgt rechtstreekse terugkoppeling van de intermediair en/of de Belastingdienst.	Gestructureerde informatie uitwisseling tussen intermediair en belanghebbende
4. Geen transparant procesverloop voor belanghebbende		Inzicht in processtatus via één kanaal
5. Beperkt hergebruik van data	Aansluiting op ERDS en publicatie van ketenspecificaties door publieke en private	Belanghebbende kan via dezelfde systematiek gegevens uitwisselen met verschillende partijen

	partijen.	(publiek en privaat) en data hergebruiken.
6. Identificatie niet op actor-niveau	Alle actoren gebruiken op individueel en/of organisatieniveau PKI.o-certificaten	Individu en betreffende organisatie identificeerbaar. De belastingdienst weet met welke actor er informatie wordt uitgewisseld.