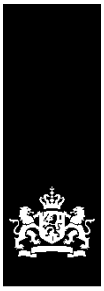
FS-20161019.09B



Analyse van het afsprakenstelsel TrustTester

Rapport van bevindingen

Colofon

Naam project	TrustTester
Versienummer	1.3 (30 augustus 2016)
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl
Bureau Forum Standaardisatie	Marijke Abrahamse
Begeleidende partij	Jasmijn Wijn en Paul Dam (VKA)
Onafhankelijk voorzitter	Wil Janssen (InnoValor)

Inhoudsopgave

Samenvatting

Toetsing

In december 2015 heeft de Regieraad Dienstverlening het Forum Standaardisatie verzocht een informele analyse te doen naar de afsprakenstelsels TrustTester en Qiy. Deze afsprakenstelsels zouden voor de overheid een oplossingsrichting kunnen bieden rondom het vraagstuk van regie op gegevens door burgers en bedrijfsleven. Het doel van de analyse is om vast te stellen in hoeverre deze stelsels platformonafhankelijk, open en robuust zijn. De analyse maakt deel uit van een reeks initiatieven van het programma RoG[1]. Het Forum Standaardisatie heeft ingestemd met dit verzoek.

TrustTester

TrustTester is een door TNO ontwikkeld technisch platform met een onderliggend afsprakenstelsel waarbij gebruikers zelf digitaal kunnen bewijzen dat de door henzelf verstrekte informatie (attributen) correct en actueel is. TrustTester is gebaseerd op validatie in plaats van verstrekking, waardoor geen gegevens worden uitgewisseld. Door de toepassing van homomorfe encryptie wordt de vercijferde data met elkaar vergeleken zonder dat de vergeleken grootheden bekend worden. Voordeel van deze methodiek is dat geen enkele betrokken partij iets leert dat hij nog niet wist en dat er geen profielen opgebouwd kunnen worden over de persoon waarvoor de validatie wordt uitgevoerd.

Geadviseerd functioneel toepassingsgebied:
TrustTester is een afsprakenstelsel voor de validatie van gegevens van burgers/consumenten en bedrijven. Het doel van deze validatie is om te bewijzen dat de door henzelf verstrekte informatie correct en actueel is.

Bevindingen

Persoonlijk Datamanagement wordt door stakeholders gezien als een belangrijke ontwikkeling, waar het zinvol is om bij aan te sluiten. Uit de analyse blijkt dat het TrustTester afsprakenstelsel zich richt op validatie en niet op gegevensverstrekking, een unieke functionaliteit biedt. TrustTester organiseert dat burgers en overheden slechts de enige noodzakelijke informatie uitwisselen: of aan benodigde eisen voor een transactie is voldaan. De inhoud van gegevens wordt niet gedeeld.

- Er is, naast TrustTester, op dit moment geen acceptabele digitale oplossing voor het gebruik van elkaars nuttige gegevens zonder dat er profielen kunnen worden opgebouwd en zonder dat er waardevolle gegevens in verkeerde handen kunnen vallen (4.2.1 Baten).
- TrustTester is nog conceptueel, wat wil zeggen dat gebruikers nog geen ervaring op hebben kunnen doen met het gebruik van het afsprakenstelsel. De conceptuele status blijkt ook uit de mate van ontwikkeling van TrustTester, dit is nog niet op alle onderwerpen van onderliggende toetsing voldoende.
- TrustTester is echter wel afhankelijk van aangesloten attribute providers; zonder deze partijen kunnen gegevens niet gevalideerd worden (k.4)[2].
- De integriteit van de validatie hangt af van het integriteitsniveau van het authenticatiemiddel, niet van TrustTester (k.7).
- Bij het ontwerp van TrustTester staat *security by design* centraal, waardoor de beveiliging van TrustTester volledig geïntegreerd is (k.6).

1 Programma "Burgers en Bedrijven in Regie over hun Gegevens", uitgevoerd in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Economische Zaken, via de Regieraad Dienstverlening van de Digicommissaris.

2 De K-nummers verwijzen naar de Kwalitietstoets in paragraaf 4.3 van dit rapport.

- Door de lineaire schaling van TrustTester kan er flexibel worden ingespeeld op een groeiend aantal toepassingen en specifieke piekmomenten (k.3).
- In het huidige model authentiseert een claimant met verschillende authenticatiemiddelen bij de relying party en de attribute provider. Hierdoor kan een switch attack plaatsvinden. Dit risico kan worden ondervangen wanneer gebruik gemaakt kan worden van Idensys. (k.6 en k.7).
- De aanstaande pilot zal uit moeten wijzen of TrustTester onder andere afdoende prestaties biedt voor alle typen gebruik (k.3) en of het stelsel voldoende stabiel is (k.5). Daarnaast dient bepaald te worden of de validatiegegevens gezien worden als persoonsgegevens in het kader van de Wbp (k.6).

Randvoorwaarden voordat inzet en gebruik plaatsvindt
Voordat gebruik van TrustTester door de overheid opportuun wordt dienen meerdere activiteiten ontplooid te worden, die moeten leiden tot een verbetering van de scores van de Kwaliteitstoets en Herbruikbaarheidstoets die voor deze analyse zijn uitgevoerd.

<u>Aanbevelingen in geval brede inzet en gebruik van TrustTester binnen de overheid aan de orde is</u>

- De expertgroep adviseert de policy enforcer per casus te beoordelen welke gegevens gevalideerd kunnen en mogen worden. Aangezien voor veel casussen een wettelijke basis geldt wordt geadviseerd om het verantwoordelijke departement hierbij te betrekken.
- De expertgroep roept de overheid om een experiment te initiëren waarin de werking van TrustTester aangetoond kan worden. Bij voorkeur is dit initiatief een toepassing van validatie tussen twee publieke organisaties. Door een actieve rol en het geven van ruimte voor innovatie ontstaat mogelijk een klimaat waarin meer initiatieven rondom TrustTester ontstaan.
- De expertgroep roept TNO en Qiy op om te bekijken binnen welke casus en organisatorisch werkingsgebied de afsprakenstelsels TrustTester en Qiy overlappen en wanneer zij in functionele, technische en/of organisatorische zin complementair aan elkaar kunnen zijn en zo de potentie van beide stelsels helder te kunnen duiden.
- De expertgroep adviseert om organisaties als Bits for Freedom mee te laten kijken en denken met de verdere ontwikkeling van TrustTester.
- De expertgroep adviseert TNO om een semantisch model op te stellen om een juiste validatie van attributen mogelijk te maken (k.4).
- De expertgroep roept daarnaast op om het speelveld breder in beeld te brengen: hoe verhouden verschillende Persoonlijk Datamanagement-voorzieningen zich, hoe verhouden zij zich tot (andere) attributendiensten en in hoeverre deze voorzieningen complementair aan elkaar kunnen worden ingezet.

1 Doelstelling rapport

1.1 Achtergrond

1.1.1 Forum Standaardisatie

Om interoperabiliteit tussen overheidsorganisaties en bedrijven, tussen overheidsorganisaties en burgers, en tussen overheidsorganisaties onderling te bevorderen zijn in 2006 het College en Forum Standaardisatie opgericht. Interoperabiliteit staat in dit verband voor het vermogen om op elektronische wijze gegevens uit te wisselen tussen organisaties. In november 2014 zijn de taken van het College Standaardisatie over gedragen aan het Nationaal Beraad Digitale Overheid. Het Forum Standaardisatie behoudt haar rollen, taken en werkwijze en adviseert nu het Nationaal Beraad.

Het Forum Standaardisatie bevordert in het kader van interoperabiliteit het gebruik van open standaarden. Het Forum Standaardisatie heeft een zorgvuldige toetsingsprocedure voor het selecteren van open standaarden die gebruikt moeten worden binnen de publieke sector. Geselecteerde standaarden komen op de zogenaamde 'pas toe of leg uit'-lijst. Sinds 2012 toetst het Forum ook e-Overheidsvoorzieningen op geschiktheid voor hergebruik. Daarnaast doet het Forum Standaardisatie uiteenlopende verkenningen en analyses naar ontwikkelingen en instrumenten in relatie tot interoperabiliteit.

Aanleiding analyse naar afsprakenstelsels TrustTester en Qiy

In december 2015 heeft de Regieraad Dienstverlening het Forum Standaardisatie verzocht een analyse te doen naar de afsprakenstelsels TrustTester en Qiy. Deze afsprakenstelsels zouden voor de overheid een oplossingsrichting kunnen bieden rondom het vraagstuk van regie op gegevens door burgers en bedrijfsleven. Doel van de analyse is vast te stellen in hoeverre deze stelsels platformonafhankelijk, open en robuust zijn. Het Forum Standaardisatie heeft ingestemd met dit verzoek.

1.1.2 Voorzieningentoets voor bestaande voorzieningen

Het Forum voorziet voor bestaande voorzieningen binnen de (semi-) publieke sector op aanvraag in onafhankelijke toetsing en opname op de Lijst getoetste voorzieningen voor hergebruik. Plaatsing op de Lijst is een status die is gericht op het bevorderen van breed gebruik. De doelgroep van de Lijst is de gehele (semi-)publieke sector. Deze omvat naast de rijksdiensten, uitvoeringsorganisaties, provincies, waterschappen en gemeenten ook instellingen in de sectoren onderwijs, zorg en sociale zekerheid. Met plaatsing op de Lijst ontstaat voor (semi-) overheidsorganisaties een incentive om voorzieningen te selecteren conform de Lijst. Ook kunnen organisaties van elkaar leren doordat de dialoog over features en eigenschappen open gevoerd kan worden, wat kan leiden tot een breder draagvlak en nieuwe toepassingen.

Een voorziening in deze context is een bouwsteen voor de elektronische overheid, die bijdraagt aan dienstverlening aan burgers, bedrijven of medeoverheden. Het is een samenstel van bijvoorbeeld informatie, organisatie en/of koppelvlak, en bevat in ieder geval een elektronische (geautomatiseerde) component.

Toetsingscriteria
In het kader van het streven naar interoperabiliteit komen voorzieningen in aanmerking voor toetsing indien:

- het een overheidsvoorziening betreft die dienstig is aan de doelen van e-overheid (zoals verbeteren dienstverlening en interne efficiency);
- de voorziening algemeen gebruikt kan worden (generieke functionaliteit en bestaande en potentiële gebruikers);
- de voorziening niet wettelijk verplicht is;
- er geen blokkerende omstandigheden zijn voor ingebruikname door nieuwe gebruikers.

Na aanmelding doorloopt de voorziening een toetsingsprocedure waarbij wordt bekeken of de voorziening voor opname op de Lijst in aanmerking komt. Het Nationaal Beraad spreekt zich uit over de voorzieningen die op de Lijst zullen worden opgenomen op basis van een beoordeling van de voorziening.

1.2 Proces toetsing TrustTester

In december 2015 heeft het Forum Standaardisatie ingestemd met het verzoek van de Regieraad Dienstverlening om op basis van de Toetsingsprocedure voor voorzieningen informele analyses uit te voeren op de afsprakenstelsels TrustTester en Qiy. Het Forum maakt voor deze analyses gebruik van de criteria en ervaring die is opgedaan met eerdere toetsing van uiteenlopende voorzieningen en afsprakenstelsels. Het betreft in dit geval echter informele analyses die niet zijn gericht op of zullen resulteren in verlenen van status dan wel plaatsing op de ijst van getoetste voorzieningen voor hergebruik.

De uitkomsten in de vorm van een rapport van bevindingen, vormen inbreng voor het programma Regie op Gegevens, en daarmee de Regieraad Dienstverlening, om te bepalen of en wat de benodigde vervolgstappen zijn om met deze stelsels verder te kunnen gaan binnen de overheid.

De analyses maken deel uit van een reeks initiatieven van het programma 'Burgers en Bedrijven in Regie over hun Gegevens' (RoG). Het programma ondersteunt de bestuurlijke en maatschappelijk dialoog over persoonlijk datamanagement (PDM). De analyses van het Forum hebben maar een beperkte scope die in de bredere context van het programma RoG beschouwd worden. Uitgebreidere toelichting op PDM, de relevantie voor de Nederlandse overheid en de ontwikkeling van afsprakenstelsels in dat kader staan beschreven in onder andere een discussiepaper[3] en een essay[4], die beide als losse bijlagen beschikbaar.

Onderhavig document heeft uitsluitend betrekking op TrustTester. Voor Qiy is dezelfde – maar een separate - procedure doorlopen. Bij de toetsing en advisering wordt het Bureau Forum Standaardisatie ondersteund door een (externe) begeleidende partij, in dit geval Verdonck, Klooster & Associates (VKA).

Het toetsingsproces van TrustTester kent de volgende stappen:

- intake en eerste toetsing aan criteria;
- uitvoering van een toets door de begeleidende partij;
- opstellen van een rapport van bevindingen door een expertgroep.

3 Discussiepaper Burger en Bedrijven in regie op hun gegevens. Discussiepaper Burger en Bedrijven in regie op hun gegevens. Versie 1.0 november 2015.

4 Persoonlijke datamanagement – Ontwikkelingen en oplossingen voor een digitale overheid. Versie 1.0 juli2016. Zie https://www.forumstandaardisatie.nl/sites/default/files/FS/2016/1019/Essay-Regie-op-Gegevens-2016.pdf

1.2.1 Doorlopen proces tot nu toe

Voor het opstellen van dit rapport van bevindingen zijn de volgende stappen doorlopen.

Intake

In de eerste plaats is een intake uitgevoerd, waarbij is beoordeeld of TrustTester getoetst kan worden met behulp van de voorzieningentoets van het Forum Standaardisatie. In de intake is door het Bureau Forum Standaardisatie en het programma Regie op Gegevens geoordeeld dat toetsing van TrustTester weliswaar afwijkt van de reguliere voorzieningentoets, maar -gezien toepasbaarheid van de Kwaliteits- en Hergebruikcriteria op 'afsprakenstelsels'- mogelijk is.

Gedurende de intake is komen vast te staan dat genoemde afwijkingen ten aanzien van de toetsing bestaan uit het volgende:

1. Dit rapport van bevindingen dient als inbreng voor het programma Regie op Gegevens, en daarmee de Regieraad Dienstverlening, er wordt geen advies voorgelegd aan het Forum Standaardisatie ter besluitvorming tot plaatsing op de Lijst,
2. Het betreft een informele toets, er volgt dus geen openbare consultatie na de expertbijeenkomst,
3. TrustTester is een afsprakenstelsel, geen ICT-voorziening,
4. TrustTester is afsprakenstelsel waarvoor vele (commerciële) toepassingen denkbaar zijn en waarbij de gebruiker (burger) centraal staat. Hierdoor staat niet op voorhand vast dat het hier om een voorziening *voor en door de overheid* gaat, sterker nog: de rol van de overheid is juist nog nader te bepalen, terwijl de voorzieningentoets van het Forum Standaardisatie tot nog toe gebruikt is voor toetsing van voorzieningen voor en door de overheid zoals MijnOverheid, eHerkenning, Digipoort PI en het Digitaal Ondernemersplein, en de informele toetsingen van SUWInet en Pleio, en
5. TrustTester is nog slechts in een beginstadium van ontwikkeling, voorheen ging het om voorzieningen die reeds volop in productie waren.

Ondanks deze afwijkingen heeft TNO, ondersteund door de begeleidende partij, gedurende de intake de zelftoets uitgevoerd, bestaande uit:

- *Kwaliteitstoets*
  Deze toets betreft de intrinsieke kwaliteit van de voorziening, en omvat aspecten als robuustheid, schaalbaarheid, en beheer.
- *Herbruikbaarheidstoets*
  Deze toets heeft betrekking op gebruiksmogelijkheden van de voorziening ook in andere domeinen dan het domein waarvoor ze is ontwikkeld.

Het resulterende document is voorgelegd aan de expertgroep.

1.3 Samenstelling expertgroep

Voor de expertgroep zijn personen uitgenodigd die vanuit hun persoonlijke expertise of werkzaamheden bij een bepaalde organisatie direct of indirect belang hebben bij het afsprakenstelsel, of die beschikken over specifieke kennis die van belang is voor beoordeling van het afsprakenstelsel. Daarnaast is een onafhankelijke voorzitter van de expertgroep aangesteld.

Bij volgende experts hebben deelgenomen aan de expertbijeenkomst:

Naam	Organisatie	Functie
Titus Sips	APG	Strategy consultant
Harmannus Kruizinga	SVB	Informatiemanager
Steven Gort	ICTU	Datafluisteraar
Frans van Koppen	Ministerie van EZ	Business architect
Esther Makaay	SIDN	Servicearchitect
Henk Duinkerken	Doorbraak in Dienstverlening	Interim manager
Eric Loe	Doorbraak in Dienstverlening	Interim manager
Floris Kleemans	Focafet	Expert UETP
André de Kok	RvIG	Stelselarchitect
Jean-Louis Roso	TNO	Senior Business Developer
Jeroen Laarakkers	TNO	Security consultant
Bram Neuteboom	Digital Me	CTO
Douwe Leguit	Ministerie van BZK	Programmamanager Regie op Gegevens
Liza Abrahamse	Ministerie van BZK	Programmamedewerker Regie op Gegevens

De rol van onafhankelijke voorzitter van de expertgroep is vervuld door Wil Janssen, managing partner bij InnoValor. De expertgroep is in opdracht van het Forum Standaardisatie begeleid door Paul Dam en Jasmijn Wijn, beide werkzaam bij Verdonck, Klooster & Associates (VKA). Marijke Abrahamse en Desiree Castillo Gosker, beide werkzaam bij het Bureau Forum Standaardisatie hebben als toehoorder deelgenomen aan de expertbijeenkomst.

1.3.1 Vervolgstappen

De bevindingen van de expertgroep zijn in een gesloten consultatie, onder de leden van het Forum Standaardisatie en de Regieraad Dienstverlening, voorgelegd voor commentaar. Na verwerking van dat commentaar – daar waar nodig worden experts wederom betrokken – is dit rapport van bevindingen opgeleverd aan het programma Regie op Gegevens, en daarmee ook aan de Regieraad Dienstverlening.

De volgende personen hebben input geleverd tijdens de gesloten consultatie:

Naam	Organisatie	Functie
Paul Zeef	Logius	Business consultant
Louis Tinselboer	Logius	Productmanager MijnOverheid
Saco Bekius	Belastingdienst	Strategisch adviseur
Jeroen Schuuring	KING	Adviseur
Mariska Zwinkels	Ministerie van OCW	Senior adviseur
Stan Dekker	Inspectie Leef-omgeving en Transport	Afdelingshoofd Procesontwerp en Vernieuwing
Marc van de Graaf	Ministerie van AZ	Adviseur
Marianne Krug	Unie van Waterschappen	Beleidsadviseur

1.4 Leeswijzer

Hoofdstuk 2 bevat een toelichting op hoofdlijnen op TrustTester. Hoofdstuk 3 bevat een weergave van de bespreking van TrustTester door de experts met als onderdelen:

- Een voorstel voor het toepassingsgebied en het werkingsgebied van TrustTester.
- Een voorstel voor aanbevelingen ter bevordering van de adoptie.

In hoofdstuk 4 zijn de bevindingen uit de toets door de begeleidende partij opgenomen. Dit hoofdstuk bevat ook de voorbeeldcasus die is opgesteld ten behoeve van de oordeelsvorming door de expertgroep.

Voor de beoordeling van TrustTester is het toetsingskader voor voorzieningen gebruikt. Hierdoor kan het voorkomen dat in onderliggend rapport gesproken wordt van een voorziening. In dit geval dient dit te worden gelezen als 'afsprakenstelsel' of 'TrustTester.

2 Toelichting op de voorziening in procedure

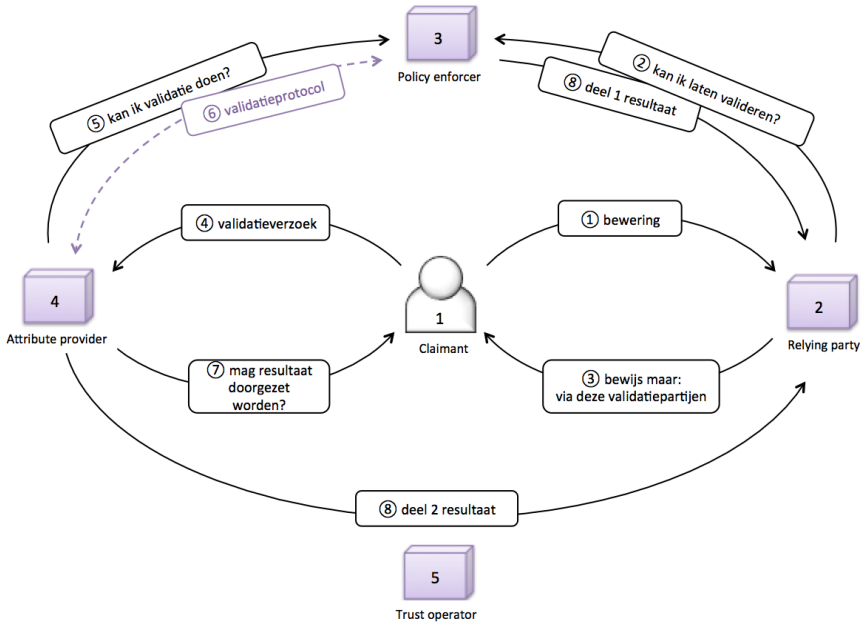
2.1 Functionaliteit

TrustTester is een technisch platform met een onderliggend afsprakenstelsel waarbij gebruikers zelf digitaal kunnen bewijzen dat door henzelf verstrekte informatie correct en actueel is. TrustTester is gebaseerd op validatie en niet op verstrekking. Gegevens (attributen) worden als zodanig niet zelf uitgewisseld, maar uitsluitend het antwoord van de validatie tegen een norm wordt uitgewisseld. Door gebruik te maken van homomorfe encryptie kan vercijferde data met elkaar worden vergeleken zonder dat de vergeleken grootheden bekend worden.

Hierdoor leert geen enkele betrokken partij iets dat hij nog niet wist, en krijgt de ontvangende partij alleen de zekerheid of een eerder afgegeven uitspraak correct is of niet. TrustTester kan zowel statische als dynamische gegevens[5] valideren.

Een eenvoudig voorbeeld van deze toepassing:
Twee miljonairs (A en B) willen bepalen wie het rijkst is, zonder elkaar te laten weten hoeveel geld zij bezitten. Beide miljonairs versleutelen de hoogte van hun vermogen met homomorfe encryptie. Vervolgens wordt een vergelijking uitgevoerd in het versleutelde domein. Het antwoord van de vergelijking wordt ook versleuteld. Uit het antwoord concluderen de miljonairs dat miljonair A het rijkst is, maar miljonair B weet niet hoe rijk miljonair A is. Ook miljonair A weet niet hoeveel geld miljonair B heeft, of hoe groot het verschil in vermogen tussen beiden is.

Conform dit voorbeeld kan een burger door middel van TrustTester bij een hypotheekverstrekking laten valideren dat het door hem verstrekte inkomensgegeven correct en actueel is. Zie voor een uitgebreidere voorbeeldcasus paragraaf 4.5.



Afbeelding 1. Schematische weergave werking TrustTester

5 Statische gegevens zijn gegevens die niet met de tijd veranderen, zoals geboortedatum en –plaats, geslacht. Dynamische gegevens veranderen daarentegen wel met de tijd, zoals leeftijd, inkomen en strafblad.

Rol	Toelichting
1. Claimant	De entiteit die iets wil laten valideren. Dit is meestal de burger/klant of een bedrijf.
2. Relying party (RP)	De partij (node) die de online dienst verleent waarvoor een attribuut gevalideerd moet worden. De dienstverlener is afhankelijk van de uitkomst van de validatie en vertrouwt hierop.
3. Policy enforcer (PE)[6]	De partij (node) die aan het begin van de transactie een transactie-ID uitgeeft. Ook controleert deze partij of de gevraagde attribuutvalidatie wel uitgevoerd mag worden. Tevens zorgt de policy enforcer voor het scheiden van de relying party (RP) en de attribute provider (AP). Deze partijen kunnen daardoor geen profiel opbouwen van de claimant.
4. Attribute provider (AP)	De partij (node) die het te valideren attribuut in zijn database heeft staan, om mee te vergelijken. Er kunnen meerdere partijen zijn die een bepaald attribuut bezitten om tegen te valideren.
5. Trust operator (TO)	De partij (node) die de voor TrustTester benodigde software ontwikkelt en beheert. Daarbij beheert de TO de koppelingspagina waarop claimants hun attribute provider kunnen selecteren en worden doorverwezen, en zorgt de TO voor de facturatie aan alle partijen die gebruik maken van het protocol. Tevens zorgt de Trust operator voor het scheiden van de relying party (RP) en de attribute provider (AP). Deze partijen kunnen daardoor geen profiel opbouwen van de claimant.

Tabel 1. Verschillende rollen binnen TrustTester

2.1.1 *Samenhang met standaarden en andere voorzieningen*

TrustTester maakt voor de validatie van gegevens gebruik van attribute providers (AP's). Voorbeelden van attribute providers zijn overheden die bronhouder zijn van basisregistraties, zoals de Basisregistratie Personen, Handelsregister, Basisregistraties Adressen en Gebouwen, Basisregistratie Voertuigen en Basisregistratie Inkomen.

Claimants maken in het authenticatieproces gebruik van voorzieningen als eHerkenning en DigiD (in het geval van publieke AP's en/of RP's) en van privaat uitgegeven authenticatiemiddelen (in geval van private AP's en/of RP's).

2.1.2 *Soortgelijke voorzieningen*

Er is een aantal voorzieningen dat functionaliteit biedt voor de gegevensuitwisseling tussen overheidsorganisaties en bedrijven. Het uitgangspunt van TrustTester is echter dat gegevens gevalideerd worden in plaats van uitgewisseld. Met deze verbijzondering van TrustTester zijn er geen soortgelijke voorzieningen bekend die gegevensvalidatie mogelijk maken zonder de verstrekking van gegevens. Hoe TrustTester in de praktijk al dan niet complementair kan worden gebruikt in combinatie met (andere) Persoonlijk Datamanagement-afsprakenstelsels, zoals Qiy en UMA, is nog niet in beeld gebracht.

6 De rol van policy enforcer wordt naar verwachting ingevuld door SIDN.

2.2 Bestaande en potentiële gebruikers

TrustTester is op dit moment nog geen werkend afsprakenstelsel, waardoor gebruikers nog geen ervaring op hebben kunnen doen met het gebruik er van. Vanuit de diverse gesprekken die TNO heeft gevoerd met zowel publieke als private partijen, en de usecases die zijn opgesteld, is een aantal potentiële gebruikers aan te merken. Deze partijen bevinden zich zowel in het publieke domein, publiek-private domein als het private domein:

- Nutsvoorzieningen
- Notariaten
- Financiële dienstverleners
- Uitzendbureaus
- Scholen
- Gezondheidszorg
- Sociale woningmarkt
- Online gokwebsites

2.3 Beheerorganisatie en governance

TNO is bedenker van het afsprakenstelsel, en aanjager van operationalisatie van TrustTester. TNO zal het operationele afsprakenstelsel niet gaan beheren. Governance is onderdeel van het experiment dat dit jaar op het programma staat.

Er is een model voorzien waarbij de policy enforcer verschillende werkgroepen organiseert voor inspraak op en doorontwikkeling van TrustTester. Attribute providers (AP's) en trust operators (TO's) kunnen deelnemen aan deze werkgroepen.

Het afsprakenstelsel wordt bekostigd vanuit een vastgesteld kostenmodel, waarbij de relying party betaalt per validatie. De diverse validaties kunnen verschillende prijzen hebben. Attribute providers (AP's) en relying parties (RP's) betalen zelf de kosten die gemaakt moeten worden om TrustTester te implementeren binnen de eigen organisatie.

2.4 Toekomstige ontwikkelingen

Verwacht wordt dat op korte termijn gestart kan worden met een pilot. Hierbij kan gedacht worden aan een pilot waarbij consumenten enkele attributen valideren die een rol spelen bij het aanvragen van een hypotheek, zoals de hoogte van het bruto-inkomen, de beschikking over een leaseauto en het hebben van een vast contract. In het experiment wordt aandacht besteed aan technische, juridische, operationele, bestuurlijke en beleidsmatige vraagstukken, zoals gebruiksvriendelijkheid, toegevoegde waarde voor de relying party en de conformiteit met bestaande wet- en regelgeving.

Een dergelijk experiment duurt ongeveer zes maanden. TrustTester is, bij een succesvol experiment, naar verwachting in 2017 beschikbaar als operationeel afsprakenstelsel.

3 Bespreking van TrustTester door de experts

3.1 Afbakening

Toelichting afbakening: functioneel toepassingsgebied en organisatorisch werkingsgebied
De toetsing van een voorziening vindt plaats tegen de achtergrond van een beoogd gebruik dat is afgebakend door:

- *Organisatorisch werkingsgebied*
  Dit het domein (organisatorisch, taakvelden) binnen de overheid waarin de voorziening wordt of kan worden toegepast. Bijvoorbeeld: gemeenten, provincies, waterschappen, Rijk, zorginstellingen of de sector werk & inkomen.
- *Functioneel toepassingsgebied*
  Dit is de omschrijving van de functie die de voorziening vervult binnen het organisatorisch werkingsgebied

Functioneel toepassingsgebied
TrustTester is een afsprakenstelsel voor de validatie van gegevens van burgers/consumenten en bedrijven. Het doel van deze validatie is om te bewijzen dat de door henzelf verstrekte informatie correct en actueel is.

Organisatorisch Werkingsgebied

Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

Bovenstaande formulering van het organisatorisch werkingsgebied is de 'standaardformulering' van het Forum Standaardisatie. De experts zien geen aanleiding om dit te beperken.

3.2 Bevinding en aanbevelingen voor inzet en gebruik van de voorziening

Persoonlijk Datamanagement wordt door stakeholders gezien als een belangrijke ontwikkeling, waar het zinvol is om bij aan te sluiten. De uitgevoerde analyse wijst uit dat het TrustTester afsprakenstelsel zich richt op validatie en niet op gegevensverstrekking, een unieke functionaliteit biedt. TrustTester organiseert dat burgers en overheden enkel noodzakelijke informatie uitwisselen: of aan benodigde eisen voor een transactie is voldaan. De inhoud van gegevens wordt niet gedeeld. Governance en andere organisatorische aspecten zijn nog in ontwikkeling.

Voor gebruik van TrustTester door de overheid geldt wel een aantal randvoorwaarden en dienen meerdere activiteiten uitgevoerd te worden.

3.2.1 Randvoorwaarde voordat inzet en gebruik plaatsvindt

Voor gebruik door de overheid geldt dat meerdere activiteiten ontplooit dienen te worden, die moeten leiden tot een verbetering van de scores van de Kwaliteitstoets en Herbruikbaarheidstoets die voor deze analyse zijn uitgevoerd.

3.2.2 Aanbevelingen die tot brede inzet en gebruik kunnen leiden

Rol van de overheid
De expertgroep roept de overheid om een experiment te initiëren waarin de werking van TrustTester aangetoond kan worden. Bij voorkeur is dit initiatief een toepassing van validatie tussen twee publieke organisaties. Door een actieve rol en het geven van ruimte voor innovatie ontstaat mogelijk een klimaat waarin meer initiatieven rondom TrustTester ontstaan.

De overheid kan in dit soort afsprakenstelsels in meerdere operationele rollen (al dan niet tegelijkertijd) participeren:

- als beheerder van bronnen van persoonlijke gegevens (zoals de basisregistraties), binnen TrustTester wordt deze rol *attribute provider* genoemd (AP),
- als partij die gegevens van burgers vraagt (zoals bij de aanvraag van toeslagen, subsidies en vergunningen), binnen TrustTester wordt deze rol *relying party* genoemd (RP).

Sturing en toezicht
Bovenstaande mogelijkheden voor operationele inzet van TrustTester brengen in min of meerdere mate met zich mee dat de overheid zich – naar onze mening – het belang moet aantrekken van het (mede) richting geven aan (de ontwikkeling van) het afsprakenstelsel TrustTester,

Daarbij komt dat indien meerdere (of zelfs vele) overheidsorganisaties TrustTester (of een dergelijk afsprakenstelsel) inzetten, de noodzaak groeit om de overheidsparticipatie in deze rollen efficiënt vorm te geven en bijvoorbeeld niet alle overheidsorganisaties direct te laten participeren in genoemde organen van het afsprakenstelsel.

Overigens laat bovenstaande onverlet dat de overheid op grond van huidige wet- en regelgeving reeds een toezichthoudende rol heeft. Deze raakt onder andere aan het feit dat Issuers, Relying Parties en Data Providers (en mogelijk ook Service Providers) persoonsgegevens verwerken. De toezichthoudende rol staat los van de verschillende opties voor operationele en/of sturende rollen die ingevuld kunnen worden en wordt in deze analyse verder niet behandeld.

Draagvlak onder burgers
De expertgroep adviseert om organisaties als Bits for Freedom mee te laten kijken en denken met de verdere ontwikkeling van TrustTester.

Overig

Te valideren gegevens
De expertgroep adviseert de policy enforcer om per casus te beoordelen welke gegevens gevalideerd kunnen en mogen worden. Aangezien voor veel casussen een wettelijke basis geldt wordt geadviseerd om het verantwoordelijke departement hierbij te betrekken.

Samenhang Qiy en TrustTester
De expertgroep roept TNO en Qiy op om te bekijken binnen welke casus en organisatorisch werkingsgebied de afsprakenstelsels TrustTester en Qiy overlappen en wanneer zij complementair aan elkaar kunnen zijn om zo de potentie van beide stelsels helder te kunnen duiden. Hierbij gaat het om

functioneel, technisch en organisatorisch perspectief. Daarnaast bestaat de behoefte aan inzicht in welke situaties Attribute Providers en Relying Parties met meerdere stelsels te maken krijgen vanwege bijvoorbeeld een eventuele overlap in functionaliteit van verschillende stelsels zoals TrustTester en Qiy.

Opzetten semantisch model
Ook dient er een semantisch model opgezet te worden voor de uit te wisselen attributen. Attributen kunnen voor relying parties en attribute providers een andere betekenis hebben en kunnen hierdoor anders worden geïnterpreteerd. Het is belangrijk dat er afspraken worden gemaakt om semantische discussies en verkeerde interpretaties te voorkomen.

4 Toetsing van de voorziening aan criteria

4.1 Inleiding

Dit hoofdstuk bevat de bevindingen uit de toets door de begeleidende partij en die derhalve deel uitmaken van de oordeelsvorming door de Expertgroep. De bevindingen bestaan uit de volgende onderdelen:

- de kwaliteitstoets en de herbruikbaarheidstoets zoals deze zijn uitgevoerd door de begeleidende partij,
- de voorbeeldcasus, en
- de evaluatie in de vorm van een kwalitatieve businesscase op hoofdlijnen.

Omwille van het overzicht is de evaluatie als eerste opgenomen.

4.2 Evaluatie (kwalitatieve businesscase)

De evaluatie vat de bevindingen uit de toets samen, en wel onder de noemers baten, kosten en risico's van inzet en gebruik van de voorziening door de overheid.

Onder baten wordt in dit verband verstaan, de voordelen van gebruik van de voorziening in termen van:

- een bijdrage aan de doelen van de e-overheid, en
- functionele bruikbaarheid: de mogelijkheid om de bedrijfsvoering te optimaliseren.

Onder kosten wordt verstaan: een kwalificatie op macroniveau van de kostenverhouding tussen enerzijds de kosten van hergebruik van de voorziening versus anderzijds de kosten van het zelf ontwikkelen van (een) soortgelijke voorziening(en) door nieuwe gebruikers.

Onder risico's wordt verstaan: mogelijke problemen bij gebruik van de voorziening, en de oorzaken van deze mogelijke problemen. Daarbij wordt ook aangegeven welke maatregel het risico kan verkleinen. De informatie in dit onderdeel is vooral afkomstig uit de samenvatting van de belangrijkste aandachtspunten die uit de kwaliteitstoets en de herbruikbaarheidstoets naar voren zijn gekomen.

Kanttekening die bij de evaluatie geplaatst dient te worden is dat TrustTester op dit moment nog in ontwikkeling is. Hierdoor kan nog niet worden gesproken van een volledig werkend afsprakenstelsel. In de toetsing is gekeken naar de huidige status van TrustTester en het potentieel van TrustTester als 'zoemend' afsprakenstelsel.

4.2.1 Baten

Bijdrage aan de doelen van e-overheid

☐ Niet aan voldaan ☐ Enigszins aan voldaan ☐ Grotendeels aan voldaan ☑ Volledig aan voldaan	Het is een doelstelling van de e-overheid om burgers en bedrijven zo makkelijk mogelijk digitaal zaken te laten doen met de overheid, waarbij digitaal zaken doen betrouwbaar, veilig en betaalbaar moet zijn. *Veilige digitale gegevensuitwisseling* Uitwisseling van gegevens vormt een toenemend probleem, omdat partijen wel gegevens willen ontvangen, maar deze niet willen verstrekken om juridische, competitieve en risicobeheersingsredenen. Met name bij digitale gegevensuitwisselingen zijn deze barrières onneembaar. Noodgedwongen wordt daarom veel informatie uitgewisseld via papier, wat buiten het digitale domein valt. Daarnaast nemen de processen om deze papieren informatiestroom te verwerken relatief veel tijd in beslag, wat resulteert in hoge kosten. Ook is de kans groot dat er (door menselijke handelingen) fouten worden gemaakt gedurende de informatieverwerking. Uitwisseling op papier (bijvoorbeeld een kopie van een legitimatiebewijs) draagt ongewenst significant bij aan de kans op identiteitsfraude. *Eenmalige gegevensverstrekking* Er zijn veel situaties denkbaar waarbij burgers/consumenten en bedrijven gegevens moeten verstrekken om een dienst af te nemen of een product aan te schaffen. De 'verkopende' partij moet deze gegevens vervolgens controleren, waarbij een burger/consument de gegevens ook hard copy moet aanleveren. Deze processen nemen relatief veel tijd in beslag, wat resulteert in hoge kosten. Daarnaast is de kans groot dat er (door menselijke handelingen) fouten worden gemaakt gedurende de informatieverwerking. Dit handmatige controleproces is echter niet noodzakelijk, aangezien er (semi-)overheden zijn die al beschikken over deze informatie en deze informatie actueel houden. In het geval van een loonverificatie beschikken het UWV en de Belastingdienst over actuele loongegevens. *TrustTester* maakt het mogelijk om de door de burger/consument verstrekte gegevens te laten verifiëren bij (semi-)overheden die al beschikken over de benodigde gegevens. Er is op dit moment geen acceptabele digitale oplossing voor het gebruik van elkaars nuttige gegevens zonder dat er profielen kunnen worden opgebouwd en zonder dat er waardevolle gegevens in verkeerde handen kunnen vallen. *TrustTester* maakt het mogelijk om digitaal gegevens (attributen) te valideren, zonder deze te verstrekken. Hierdoor kunnen geen profielen worden opgebouwd van de claimant (burger of consument) en is de gevalideerde informatie niet alleen betrouwbaar, maar ook veilig.

Functionele bruikbaarheid

☐ Niet aan voldaan ☐ Enigszins aan voldaan ☐ Grotendeels aan voldaan ☑ Volledig aan voldaan	*TrustTester* maakt het mogelijk dat (overheids)organisaties gestructureerd gegevens van burgers/consumenten en bedrijven kunnen valideren. Het gebruik van *TrustTester* is voor meerdere toepassingen denkbaar. Generiek is *TrustTester* bruikbaar bij de afname van producten of diensten waar voorafgaand gegevensvalidatie nodig is. Voorbeelden zijn het realtime valideren van een VOG-status, validatie van inkomensgegevens, en het online aanschaffen van producten of diensten waar leeftijdsvalidatie nodig is.

4.2.2 *Kosten*

Relatieve kosten (macro) bij hergebruik zijn lager dan bij het uitblijven van hergebruik

☐ Niet aan voldaan ☐ Enigszins aan voldaan ☐ Grotendeels aan voldaan ☑ Volledig aan voldaan	Met betrekking tot de kosten betalen de 'early adaptors' de meeste kosten. Dit komt doordat deze gebruikers de kosten voor het eenmalig realiseren van een technisch platform en het afsprakenstelsel moeten dragen. Attribute providers en relying parties dragen daarnaast zelf de kosten voor het implementeren (en gebruiken) van *TrustTester*.

4.2.3 *Risico's*

Onderdeel van de pilot is om te kijken welke technische, organisatorische, juridische, financiële en overige risico's zich voor (kunnen) doen, wat de impact is van deze risico's en welke maatregelen genomen moeten worden om deze risico's weg te nemen.

Technische risico's	
Oorzaak	1. TrustTester is afhankelijk van de beschikbaarheid van de databronnen van de attribute provider en de beschikbaarheid van identificatie- en authenticatiemiddelen van de attribute provider en de relying party. 2. De identiteit van een claimant bij een relying party is niet gelinkt aan de identiteit van een claimant bij de attribute provider.
Gevolg (kans en impact)	1. Op dit moment zijn geen kritieke validaties voorzien die een hoge beschikbaarheid van de databron vereisen. 2. Een switch attack is mogelijk, waarbij twee verschillende claimants samenwerken om een validatie te bewerkstelligen die het gewenste resultaat oplevert.
Mogelijke maatregel	1. Kwaliteitsnormen en testen van releases op hoog niveau vasthouden. 2. Door de identificerende gegevens zoals een sessie ID mee te versleutelen wordt de kans verkleind dat persoonsverwisseling kan plaatsvinden. Hoe meer identificerende gegevens worden toegepast voor dit doel, des te kleiner de kans op persoonsverwisseling is.
Onderdeel van het experiment is om te kijken welke technische risico's zich voor (kunnen) doen, wat de impact is van deze risico's en welke maatregelen genomen moeten worden om deze risico's weg te nemen.	

In de toekomst kan TrustTester gebruik maken van Idensys, een eID-middel. Hierdoor hoeft een claimant niet meer in te loggen met verschillende authenticatiemiddelen waardoor een switch attack niet meer mogelijk is.

Organisatorische risico's	
Oorzaak	De afhankelijkheid van de policy enforcer en trust operator is groot waardoor de policy enforcer 24/7 beschikbaar moet zijn.
Gevolg (kans en impact)	Als de policy enforcer of de trust operator niet beschikbaar is kan de verificatie van gegevens door middel van TrustTester niet worden afgerond. In het huidige ontwerp is de rol van policy enforcer toebedeeld aan SIDN. De stabiliteit van SIDN (als policy enforcer) staat momenteel niet ter discussie.
Mogelijke maatregel	-
Belangrijk aandachtspunt is wel dat de 'schade' van het niet beschikbaar zijn van de databron of de policy enforcer afstraalt op de relying party, omdat het validatieproces op dat moment niet kan worden afgerond.	

Kwaliteitsrisico's	
Oorzaak	TrustTester is afhankelijk van de kwaliteit van de databronnen van de attribute provider.
Gevolg (kans en impact)	De kwaliteit van de databronnen bepaalt de mate van betrouwbaarheid van de data.
Mogelijke maatregel	Kwaliteitsnormen stellen voor de attribute provider, ook in de selectie van attribute providers. Het gewenste niveau van betrouwbaarheid en dus te selecteren attribute provider kan per validatie verschillen. De claimant ziet eerst het resultaat van de validatie voordat het aan de relying party wordt doorgegeven. Foutieve of onverwachte uitkomsten kunnen zo door de claimant worden gesignaleerd (dit kan tevens aanleiding geven tot correctie). De relying party kan met TrustTester meerdere attribute providers dezelfde validatie uit laten voeren. Gelijkluidende resultaten verkleinen de kans op onjuiste resultaten die worden veroorzaakt door fouten in de bron.
Oracle heeft aangegeven de functionaliteit van TrustTester direct in de eigen software in te willen bouwen. Dit is voor (toekomstige) gebruikers van Oracle een positief signaal, aangezien zij daardoor geen technisch platform hoeven te bouwen. Hierdoor ontstaat echter ook het risico van een 'vendor lock in'. Wanneer gebruikers van Oracle software en TrustTester in de toekomst willen overstappen naar een andere leverancier moeten zij alsnog een technisch platform (laten) bouwen om gebruik te kunnen blijven maken van TrustTester.	

4.3 Kwaliteitstoets

Onderstaande tabel bevat de score van het afsprakenstelsel op de kwaliteitscriteria. TrustTester is op dit moment nog in ontwikkeling, waardoor nog niet gesproken kan worden van een werkend afsprakenstelsel. De huidige staat van ontwikkeling van TrustTester is in de kwaliteitstoets gescoord. Dit heeft impact op de scoring van TrustTester op de kwaliteitscriteria. Vanuit dit perspectief dient de scoring van bovengenoemde criteria als '*niet aan voldaan*' of '*enigszins aan voldaan*' gelezen te worden als '*(nog) niet aan voldaan*' en '(*nog) niet volledig aan voldaan*'.

In het aanstaande experiment (zie paragraaf 4.5) wordt TrustTester getest op werking en wordt getracht openstaande vraagstukken te beantwoorden. Het experiment kan veel toegevoegde waarde hebben voor de beoordeling van een aantal criteria van de kwaliteitstoets. Dit geldt met name voor de volgende criteria:

- Onderhoudbaarheid (K.2)
- Prestaties (K.3)
- Stabiliteit (K.5)
- Beveiliging (K.6)
- Beheer (K.9)
- Actualiteit (K.10)
- Controleerbaarheid (K.11)
- Compliancy (K.12)
- Governance (K.15)

K.1.Typering

Het karakter van de voorziening is afgebakend.

☐ Niet aan voldaan ☐ Enigszins aan voldaan ☐ Grotendeels aan voldaan ☑ Volledig aan voldaan	TrustTester biedt functionaliteit voor de validatie van gegevens van burgers/consumenten en bedrijven. Het doel van deze validatie is om te bewijzen dat de door henzelf verstrekte informatie correct en actueel is. Zowel (semi-)overheden als bedrijven kunnen de rol van dienstverlener (relying party) hebben.

K.2.Onderhoudbaarheid

De voorziening is goed gedocumenteerd, zowel qua hardware als software goed onderhoudbaar, modulair opgezet en bij de (door-)ontwikkeling worden expliciete kwaliteitsnormen aangaande onderhoudbaarheid gehanteerd.

☐ Niet aan voldaan ☑ Enigszins aan voldaan ☐ Grotendeels aan voldaan ☐ Volledig aan voldaan	De huidige documentatie over TrustTester past bij de huidige levensfase van TrustTester: conceptueel en voor zover op dit moment relevant en noodzakelijk. In het aanstaande experiment wordt ontwerpdocumentatie en beperkte gebruiks- en beheerdocumentatie opgesteld. Ontwerpbesluiten worden gedocumenteerd. De software moet nog worden ontwikkeld. Hier kan zodoende geen uitspraak over worden gedaan. Wel wordt tijdens het experiment aandacht besteed aan de backwards compatibiliteit van het afsprakenstelsel.

K.3. Prestaties

De voorziening biedt afdoende prestaties voor alle typen gebruik bij de gevraagde belasting.

☐ Niet aan voldaan ☑ Enigszins aan voldaan ☐ Grotendeels aan voldaan ☐ Volledig aan voldaan	TrustTester is lineair geschaald. Hierdoor kan flexibel ingespeeld worden op een groeiend aantal toepassingen en specifieke piekmomenten. Een hogere belasting van het afsprakenstelsel heeft voor zover bekend geen invloed op de prestatie van TrustTester. Er zijn echter wel toepassingen denkbaar die invloed kunnen hebben op de prestatie. Voorbeeld hiervan is de vergelijking van foto's en video's in het kader van opsporing. Hier is meer rekenkracht voor nodig. De relying party (RP) zal als 'klant' eisen stellen aan de beschikbaarheid van de databronnen van de attribute provider (AP). Prestatie is onderdeel van het experiment.

K.4.Schaalbaarheid

De voorziening is door middel van een beheerst proces schaalbaar.

☐ Niet aan voldaan ☑ Enigszins aan voldaan ☐ Grotendeels aan voldaan ☐ Volledig aan voldaan	TrustTester vereist het gebruik van identificatie- en authenticatiemiddelen bij de relying party. Alleen op deze manier kan met enige zekerheid worden vastgesteld of de persoon die de validatie van zijn of haar gegevens wil uitvoeren ook daadwerkelijk deze persoon is. Als relying parties nog geen gebruik maken van identificatie- en authenticatiemiddelen moet dit worden ingebouwd alvorens gebruik kan worden gemaakt van TrustTester. Dit kost zowel tijd als geld. In de voorbereiding van het experiment is gebleken dat de kosten voor het aansluiten van een attribute provider relatief hoger zijn dan bij het aansluiten van een relying party. Attribute providers moeten een koppeling maken tussen de eigen database en TrustTester. Ook moet de versleuteling in de eigen TrustTester-node ingeregeld worden. TrustTester is echter wel afhankelijk van aangesloten attribute providers; zonder deze partijen kunnen gegevens niet gevalideerd worden. Ook dient er een semantisch model opgezet te worden voor de uit te wisselen attributen. De attributen 'inkomen' en 'loon' kunnen voor zowel relying parties en attribute providers een andere betekenis hebben en kunnen hierdoor anders worden geïnterpreteerd. Het is belangrijk dat er tussen relying parties en attribute providers afspraken worden gemaakt om semantische discussies en verkeerde interpretaties te voorkomen.

K.5.Stabiliteit

Van de voorziening is bekend dat deze min of meer storingsvrij kan functioneren.

☐ Niet aan voldaan ☑ Enigszins aan voldaan ☐ Grotendeels aan voldaan ☐ Volledig aan voldaan	De stabiliteit van TrustTester, wat kan worden beschouwd als een voorwaarde voor een dergelijke validatiedienst, is afhankelijk van de stabiliteit van de policy enforcer en de trust operator. Als de policy enforcer of de trust operator niet beschikbaar is kan de validatie van gegevens door middel van TrustTester niet worden afgerond. In het huidige ontwerp is de rol van policy enforcer toebedeeld aan SIDN. De stabiliteit van SIDN staat momenteel niet ter discussie. De voorspelbaarheid van gebruikstoepassing zit bij de relying party. Zij kunnen inschatten of de aankomende periode piekbelasting wordt verwacht. Indien dit het geval is zal de capaciteit van TrustTester opgeschaald moeten worden om grote verstoringen voorkomen kunnen worden. Onderdeel van het experiment is het testen van de stabiliteit op technisch niveau. Hierbij wordt ook gekeken of TrustTester bestand is tegen verkeerd gebruik. Business continuïteit is (nog) geen onderdeel van het experiment.

K.6. Beveiliging

De voorziening heeft passende beveiligingsfuncties, er is een managementsysteem voor de beveiliging dat periodiek wordt geaudit en penetratietests vinden periodiek plaats.

☐ Niet aan voldaan ☑ Enigszins aan voldaan ☐ Grotendeels aan voldaan ☐ Volledig aan voldaan	Bij het ontwerp van TrustTester staat *security by design* centraal, waardoor de beveiliging van TrustTester volledig geïntegreerd is. De policy enforcer (PE), trust operator (TO), relying party (RP) en attribute provider (AP) authenticeren door middel van PKI Signing, waardoor de partijen zeker weten dat zij daadwerkelijk aan de juiste partijen (validatie)informatie verstrekken. Authenticatie vindt plaats door middel van DigiD of een eigen authenticatiemiddel van een organisatie (bijvoorbeeld inloggegevens van internetbankieren). Een claimant (burger/consument/bedrijf) logt twee keer in: bij de relying party en bij de attribute provider. De identiteit van de claimant bij de relying party is nog niet gelinkt aan de identiteit van de claimant bij de attribute provider. Hierdoor is een switch attack mogelijk, waarbij twee verschillende claimants samenwerken om een validatie te bewerkstelligen die het gewenste resultaat oplevert. Door de identificerende gegevens zoals een sessie ID mee te versleutelen wordt de kans verkleind dat persoonsverwisseling kan plaatsvinden. In de toekomst kan TrustTester gebruik maken van Idensys, waardoor de claimant niet meer hoeft in te loggen met verschillende middelen en een switch attack niet meer mogelijk is. Penetratietesten (crystal box) zijn onderdeel van het experiment. De mate van beveiliging is ook onderdeel van

	de acceptatiecriteria van de bij het experiment betrokken partijen. Tijdens het experiment wordt gekeken naar de beleidsvraag of de validatiegegevens gezien worden als persoonsgegeven. De verwerking van persoonsgegevens stelt hogere eisen aan de beveiliging (en archivering). Het gebruik van TrustTester heeft geen invloed op de relatie tussen een organisatie in de rol van attribute provider en de ICT-leverancier van de betreffende organisatie. In diverse baselines zoals de Baseline Informatiebeveiliging Rijksdienst (BIR), Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en de Baseline Informatiebeveiliging Waterschappen (BIWA) zijn beveiligingseisen opgenomen waar overheden aan moeten voldoen in het kader van informatiebeveiliging. De beveiliging kan worden voorzien van een ISMS/ISO:27001-certificering.

K.7.Gegevensintegriteit

De voorziening garandeert de integriteit van de gedeelde gegevens.

☐ Niet aan voldaan ☑ Enigszins aan voldaan ☐ Grotendeels aan voldaan ☐ Volledig aan voldaan	Zoals bij K.6.Beveiliging beschreven logt de claimant bij zowel de relying party als bij de attribute provider in, waardoor een persoonsverwisseling tussen de inlogsessies plaats kan vinden. De relying party wil in dit voorbeeld het attribuut van persoon A valideren, terwijl de attribute provider een attribuut van persoon B valideert. De relying party gaat er echter vanuit dat de attribute provider het attribuut van persoon A heeft gevalideerd. Dit heeft zodoende niet zozeer invloed op de integriteit van de gevalideerde gegevens, maar op de betrouwbaarheid van de gevalideerde gegevens. In de toekomst kan TrustTester gebruik maken van Idensys, waardoor de claimant niet meer hoeft in te loggen met verschillende middelen en een switch attack niet meer mogelijk is. De integriteit van de validatie hangt af van het integriteitsniveau van het authenticatiemiddel, niet van TrustTester.

K.8.Standaardisatie

Er zijn weloverwogen keuzes gemaakt over de toe te passen standaarden.

☐ Niet aan voldaan ☐ Enigszins aan voldaan ☑ Grotendeels aan voldaan ☐ Volledig aan voldaan	Het uitgangspunt is dat de burger het attribuut zo makkelijk mogelijk moet kunnen leveren. Zodoende wordt voor TrustTester zoveel mogelijk gebruik gemaakt van open standaarden. TrustTester past op dit moment de volgende standaarden toe: SAML, UETP, XBRL, PDF/A, TLS, IPv6 (en diens voorganger IPv4). Er wordt op dit moment nog gesproken over een

	ontologisch model om gegevens te kunnen verwerken. Hiervoor zal gebruik worden gemaakt van verplichte standaarden zoals SKOS, RDF, OWL. Overige momenteel verplichte standaarden zijn op dit moment niet van toepassing.

K.9.Beheer

De voorziening wordt beheerd door een professionele beheerorganisatie.

☑ Niet aan voldaan ☐ Enigszins aan voldaan ☐ Grotendeels aan voldaan ☐ Volledig aan voldaan	De inrichting van de beheerorganisatie is onderdeel van het experiment. Op basis van de ervaringen uit het experiment wordt gekeken welke afspraken gemaakt moeten worden in het kader van beheerprocessen, verantwoordelijkheden, service levels etc.

K.10.Actualiteit

Aangetoond is dat de voorziening de actualiteit van gegevens en diensten realiseert die vereist en vastgelegd is.

☐ Niet aan voldaan ☑ Enigszins aan voldaan ☐ Grotendeels aan voldaan ☐ Volledig aan voldaan	De eisen aan de actualiteit kunnen per casus verschillen. De mogelijkheid voor variabele actualiteitsniveaus wordt als specificatie gebouwd en getest in het experiment, waarbij wordt gekeken of het noodzakelijk is om een extra eis te stellen aan de actualiteit van de te valideren gegevens. Voorbeeld: een loongegeven mag niet ouder zijn dan zes maanden. Bij een casus kan ook de benodigde actualiteit ook de te bevragen attribute provider bepalen. Voorbeeld: het UWV bezit meer actuele loongegevens dan de Belastingdienst. De mogelijkheid om steekproeven uit te voeren wordt ingebouwd, zodat de relying party en de attribute provider kunnen toetsen of de policies en licenties nog actueel zijn.

K.11.Controleerbaarheid

De voorziening is controleerbaar.

☑ Niet aan voldaan ☐ Enigszins aan voldaan ☐ Grotendeels aan voldaan ☐ Volledig aan voldaan	Logging is op dit moment niet ingericht bij TrustTester. De rollen en te loggen activiteiten per rol zullen na het experiment worden uitgewerkt. De verwachting is dat de relying party, attribute provider, trust operator en policy enforcer wel de afzonderlijke activiteiten zullen loggen. De logging is pas leesbaar/bruikbaar als de logging van alle vier de partijen wordt samengevoegd. Het loggen van de geleverde gegevens en de gegevens over de betrokken partijen worden niet gelogd, dit druist tegen het concept van TrustTester in.

K.12.Compliancy

De voorziening voldoet aan de wettelijke vereisten. Dit is aangetoond en hier wordt verantwoording over afgelegd.

☑ Niet aan voldaan ☐ Enigszins aan voldaan ☐ Grotendeels aan voldaan	In het experiment zal expliciet aandacht worden besteed aan de beleidsvraag of de gegevensvalidatie in het kader van de Wet bescherming persoonsgegevens (Wbp) wordt

☐ Volledig aan voldaan	gezien als verstrekking of validatie van het persoonsgegeven. Indien het wordt gezien als verstrekking van persoonsgegevens zal TrustTester conform het normenkader van de Wbp moeten worden ingericht en beheerd. De attribute provider (AP) moet conform geldende wet- en regelgeving kunnen aangeven dat zij een verstrekking van het validatieresultaat met toestemming van de burger heeft gedaan. De policy enforcer (PE) bespreekt met relying parties (RP) welke informatie benodigd is voor een validatie. Een policy enforcer mag niet meer gegevens 'verstrekken' dan strikt noodzakelijk voor de validatie. De expertgroep adviseert de policy enforcer per casus te beoordelen welke gegevens gevalideerd kunnen en mogen worden. Aangezien voor veel casussen een wettelijke basis geldt wordt geadviseerd om het verantwoordelijke departement hierbij te betrekken. TrustTester is door middel van een mini PIA getoetst door de Radboud Universiteit als lid van het PI.lab.

K.13.Interoperabiliteit

De organisatorische, semantische, technische en juridische interoperabiliteit is zodanig dat hergebruik niet wordt belemmerd.

☐ Niet aan voldaan ☑ Enigszins aan voldaan ☐ Grotendeels aan voldaan ☐ Volledig aan voldaan	TrustTester is niet organisatiespecifiek. Het gebruik van TrustTester is echter niet automatisch semantisch interoperabel. Het is de vraag of dit binnen TrustTester opgelost moet worden of dat de gebruikers (attribute provider en relying party) dit samen op moeten lossen. Bij 'K.8.Standaardisatie' is beschreven van welke verplichte open standaarden TrustTester gebruik maakt. Aanvullend wordt gebruik gemaakt van een secure data comparing protocol voor de vergelijking van attributen. Dit is een open en gepatenteerd protocol, maar het is geen standaard.

K.14.Certificering

Kwaliteit is mede door certificering gegarandeerd.

☐ Niet aan voldaan ☑ Enigszins aan voldaan ☐ Grotendeels aan voldaan ☐ Volledig aan voldaan	De trust operator zou gecertificeerd kunnen worden/zijn, bijvoorbeeld ISO:9001 en/of ISO:27001.

K.15.Governance

De governance is in overeenstemming met de reikwijdte van het gebruik van de voorziening.

☐ Niet aan voldaan ☑ Enigszins aan voldaan ☐ Grotendeels aan voldaan ☐ Volledig aan voldaan	Het governancemodel wordt na afronding van het experiment uitgewerkt. Er is een model voorzien waarbij de policy enforcer[7] verschillende werkgroepen organiseert voor inspraak op en doorontwikkeling van TrustTester. Attribute providers (AP's) en trust operators (TO's) kunnen deelnemen aan deze werkgroepen. Ook is een raad van toezicht voorzien.

4.4 Herbruikbaarheidstoets

Onderstaande tabel bevat de score van het afsprakenstelsel op de criteria voor herbruikbaarheid.

Zoals ook aangegeven bij de kwaliteitstoets (zie paragraaf 4.3) is voor de herbruikbaarheidstoets de huidige staat van ontwikkeling van TrustTester gescoord. In het aanstaande experiment (zie paragraaf 4.5) wordt TrustTester getest op werking en wordt getracht openstaande vraagstukken te beantwoorden. Het experiment kan veel toegevoegde waarde hebben voor de beoordeling van een aantal criteria van de herbruikbaarheidstoets. Dit geldt met name voor de volgende criteria:

- Functionaliteit (H.2)
- Financiering (H.3)

H.1.Nut en noodzaak

Het karakter van de voorziening is afgebakend en het nut van de voorziening op landelijk niveau wordt breed gedragen.

☐Niet aan voldaan ☑Enigszins aan voldaan ☐Grotendeels aan voldaan ☐Volledig aan voldaan	Het karakter van TrustTester is voldoende afgebakend: het biedt de functionaliteit voor de validatie van gegevens van burgers/consumenten en bedrijven. Het doel van deze validatie is om aan te tonen dat een burger/consument of bedrijf in aanmerking komt voor de afname van een product of dienst. Vanuit de diverse gesprekken die TNO heeft gevoerd met zowel publieke als private partijen, en de usecases die zijn opgesteld zijn voldoende positieve signalen afgegeven over toekomstig gebruik van het afsprakenstelsel. Zowel publieke als private partijen zien mogelijkheden voor de toepassing van TrustTester, zowel in de rol van relying party als attribute provider. De expertgroep geeft aan dat er ook ervaring met TrustTester opgedaan kan worden door de validatie van gegevens/gegevensuitwisseling tussen (semi-)overheidsorganisaties. Bijvoorbeeld organisaties in de SUWI-keten. Een dergelijke 'pilot' kan als voorbeeld gelden voor andere organisaties.

7 De rol van policy enforcer wordt naar verwachting ingevuld door SIDN.

	Het is op dit moment niet duidelijk of het gebruik van TrustTester resulteert in een afname van administratieve lasten. Dit kan een direct resultaat zijn van de tijdswinst die wordt gerealiseerd door de relying party. Mogelijk nemen de administratieve lasten voor de attribute provider toe, met bijbehorende kosten, terwijl de financiële baten toekomen aan de relying party. Hier kunnen echter wel maatschappelijke baten voor de relying party tegenover staan. De baten van gebruik kunnen ook per casus verschillen.

H.2.Functionaliteit

De functionaliteit bevat geen essentiële lacunes voor de doelgroep van de voorziening. Toekomstvastheid van de voorziening is geborgd met een procedure voor aanpassing en uitbreiding van de voorziening.

☐Niet aan voldaan ☑ Enigszins aan voldaan ☐Grotendeels aan voldaan ☐Volledig aan voldaan	De doelgroep van TrustTester bestaat uit publieke en private partijen die gegevens willen valideren in opdracht van een burger/consument of bedrijf. De basisfunctionaliteit is generiek, maar kan aangevuld worden indien een toepassing dit vereist. Na afronding van het experiment zal de wijze waarop uitbreiding en ontwikkeling van het afsprakenstelsel plaatsvindt beschreven worden in standaardprocedures voor wijzigingen (changemanagement).

H.3.Financiering

Er is geen risico voor het voortbestaan van de voorziening door het ontbreken van financiering.

☐Niet aan voldaan ☐Enigszins aan voldaan ☑ Grotendeels aan voldaan ☐Volledig aan voldaan	Structurele financiering van TrustTester is nog niet georganiseerd. Het is nog de vraag welk deel het afsprakenstelsel structureel gefinancierd moet worden. Met betrekking tot de kosten betalen de 'early adaptors' de meeste kosten. Dit komt doordat deze gebruikers de kosten voor het eenmalig realiseren van een technisch platform en het afsprakenstelsel moeten dragen. Attribute providers en relying parties dragen daarnaast zelf de kosten voor het implementeren (en gebruiken) van TrustTester.

4.5 Voorbeeldcasus

Om in de discussie tijdens de expertbijeenkomst meer concreet te zijn over de aspecten van herbruikbaarheid wordt een voorbeeldcasus gebruikt. De casus is aangereikt door TNO. Het gaat om de volgende casus:

Aanleiding – huidige situatie zonder gebruik van TrustTester
Jaarlijks worden 200.000 hypotheken verstrekt. Op dit moment wordt door hypotheekverstrekkers veelvuldig gewerkt met online digitale omgevingen waarop (potentiële) klanten gegevens invullen. Wanneer daadwerkelijk een hypotheek wordt aangevraagd dienen allerlei semi-analoge bestanden aan de hypotheekverstrekker te worden overlegd, zoals een loonstrook en een werkgeversverklaring. Deze bestanden worden vervolgens door een medewerker van de hypotheekverstrekker handmatig op echtheid gecontroleerd en verder verwerkt. Geschat wordt dat alleen al het handmatig controleren en verwerken van een werkgeversverklaring op jaarbasis ongeveer € 20.000.000 kost.[8] De huidige doorlooptijd van een hypotheekaanvraag is circa zes weken. Dit wordt door de branche als problematisch ervaren.

Voorbeeldcasus – situatie met gebruik van TrustTester
Het TrustTester-validatiestelsel kan worden ingezet om een digitaal bewijs aan te leveren dat de door een consument ingevulde gegevens in een hypotheekaanvraag ook daadwerkelijk correct zijn. Onder andere persoons- en inkomensgegevens zijn in deze casus relevant, overheidsorganisaties die over dit type gegevens beschikken kunnen als attribute provider benaderd worden. Hierdoor kan de hypotheekverstrekker, in de rol van relying party, de gegevens direct digitaal overnemen en is verdere handmatige controle overbodig. Naast een kostenbesparing is ook tijdswinst mogelijk.

8 De kosten van de verwerking worden geschat op € 100,- per hypotheekaanvraag. Uitgaande van 200.000 hypotheekaanvragen per jaar kost de totale verwerking € 20 miljoen. Bron: Handig!.

5 Bronnen

1. TT Kernteam LAK def.
2. Eindnotitie TrustTester POC project, versie 0.9, TNO, 2014.
3. Projectplan Trial Trusttester als validatieplatform voor hypotheekverstrekking.
4. Trusttester - online waardecreatie door validatie van informatie, TNO, februari 2015.
5. Connectiemodel TrustTester 2.0, Auxilium, november 2015.
6. Discussiepaper Burger en Bedrijven in regie op hun gegevens. Versie 1.0 november 2015.
7. Persoonlijke datamanagement – Ontwikkelingen en oplossingen voor een digitale overheid. Versie 1.0 juli 2016.