



notitie

Forum Standaardisatie

www.forumstandaardisatie.nl
forumstandaardisatie@logius.nl

Bureau Forum
Standaardisatie

gehuisvest bij Logius

Postadres

Postbus 96810

2509 JE Den Haag

Bezoekadres

Wilhelmina van Pruisenweg 52

2595 AN Den Haag

Bij bezoek aan Logius is

legitimatie verplicht

FORUM STANDAARDISATIE 19 oktober 2016

Agendapunt 9. Informele analyses Qiy en TrustTester

Stuknummer 9. Oplegnotitie

Van:	Bureau Forum Standaardisatie
Aan:	Forum Standaardisatie
Bijlagen:	Geen

Resultaten informele analyses van de afsprakenstelsels Qiy en TNO TrustTester.

Ter kennisname

1. Aanleiding en aanpak

In december 2015 heeft de Regieraad Dienstverlening het Forum Standaardisatie verzocht een informele analyse uit te voeren op 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 RoG¹. Het Forum Standaardisatie heeft ingestemd met dit verzoek.

Het Forum maakte 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

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.

gericht op of zullen resulteren in verlenen van status dan wel plaatsing op de ijs 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.

2. Samenvatting van de resultaten

Analyse QIY

Typering:

Qiy biedt de mogelijkheid om de burger regie te laten voeren over de uitwisseling van gegevens – die hem betreffen – tussen verschillende organisaties. Daartoe bevat de persoonlijke Qiy Node, van waaruit gegevens worden uitgewisseld, verwijzingen naar persoonlijke gegevens. De Qiy Node bevat zelf praktisch geen gegevens. Het uitwisselen van gegevens via de persoonlijke Qiy Node gebeurt doordat de burger via zijn Qiy Node partij A laat antwoorden op een vraag/vragen van partij B. Het antwoord is beschikbaar gedurende een van tevoren bepaalde termijn.

De wereldwijd in ontwikkeling zijnde alternatieven voor Qiy zijn in deze analyseesignaleerd maar niet vergeleken.

Bevindingen

- Persoonlijk datamanagement wordt door stakeholders gezien als een belangrijke ontwikkeling, waar het zinvol is om bij aan te sluiten. Uit de analyse van het Qiy afsprakenstelsel blijkt de toegevoegde waarde van deze benadering en een serieuze belangstelling bij meerdere overheidspartijen. Voordat Qiy door de overheid ingezet zou kunnen worden moet nog wel aan een aantal randvoorwaarden voldaan worden.
- Aandachtspunt is dat het concept van zelfmanagement van persoonlijke gegevens via een node betekent dat er clustering van toegang tot een veelheid van gegevens van één individu plaatsvindt. In traditionele registers is sprake van toegang tot één of enkele gegevens van een veelheid van individuen. De impact van zo'n kanteling, met name met betrekking tot beveiligingsrisico's dient goed onderzocht te worden.
- Er is nog geen implementatie van Qiy. De toetsing heeft zich daarom beperkt tot het afsprakenstelsel en heeft zich niet gericht op een concrete implementatie. Een aantal aspecten kon daarom ook nog niet getoetst worden (o.a. K2, 3, 4 en 5 uit de Kwaliteitstoets)
- Een deel van de documentatie van het afsprakenstelsel is vrij beschikbaar, met name het beheermodel (governance). De overige documentatie is nog niet vrijgegeven.
- Qiy is aanvullend aan diensten voor verificatie van de identiteit en bijbehorende gegevens. Bijvoorbeeld toepassing in combinatie met Idensys zou mogelijk kunnen zijn.

Randvoorwaarden voordat inzet en gebruik plaatsvindt

De expertgroep benoemt de volgende zaken:

- de overheid zou het mogelijk moeten maken dat burgers hun identiteitsgegevens kunnen koppelen aan hun persoonlijke Qiy Node (burgers hebben in de huidige situatie geen beschikking over hun eigen identiteitsgegevens, ze hebben slechts inzage- en correctierecht, wat onvoldoende geschikt is om tot koppeling met Qiy te dienen);
- het zou in beginsel niet moeten gaan om het delen van 'heel gevoelige gegevens'²;
- er dient een voorziening te zijn waarmee burgers, zoals bij 'identiteitsdiefstal' en gehackt zijn of faillissement van de Issuer, hun Qiy Node kunnen terugclaimen;
- voordat gebruik door de overheid opdoort, dienen betere scores behaald te zijn op de criteria uit de Kwaliteitstoets en de Herbruikbaarheids-toets die in het kader van deze analyse uitgevoerd zijn.

Aanbevelingen in geval breed gebruik van Qiy binnen de overheid aan de orde is

Indien de overheid het afsprakenstelsel in gebruik wil nemen, dienen ten minste de volgende activiteiten uitgevoerd te worden:

- het regelen van structurele financiering van het afsprakenstelsel;
- het stellen van kaders met betrekking tot welke gegevensuitwisselingen in welke situaties juridisch (en maatschappelijk) toelaatbaar zijn³;
- huidige voorzieningen van de overheid geschikt maken voor aansluiting op Qiy;
- het initiëren van concrete toepassingen die zorgen voor een stimulerende werking;
- het organiseren van actieve en structurele participatie van de overheid in de governance van het afsprakenstelsel;
- het oproepen van TNO en Qiy 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 om zo de potentie van beide stelsels helder te kunnen duiden;
- onderzoeken op welke wijze MijnOverheid en Qiy kunnen samenwerken, waaronder de mogelijkheid om Qiy-functionaliteit(en) in MijnOverheid te brengen;
- 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.

Het rapport van bevindingen Qiy 1.3 kunt u downloaden van <https://www.forumstandaardisatie.nl/sites/default/files/FS/2016/1019/FS-20161019.09A-Rapport-van-bevindingen-Qiy-1.3-0.pdf>

² Zoals bijzondere persoonsgegevens (gezondheid, geloofsovertuiging, BSN etc.).

³ Om de kans te beperken dat organisaties de verstrekte gegevens ook voor andere doeleinden kunnen gebruiken, zoals risicoselectie.

Analyse TrustTester

Typering

TrustTester is een door TNO ontwikkeld technisch platform met een onderliggend afsprakenstelsel waarbij gebruikers digitaal kunnen bewijzen dat de door henzelf verstrekte informatie correct en actueel is. TrustTester is gebaseerd op validatie in plaats van verstrekking, met andere woorden een betrouwbare partij bevestigt dat je aan benodigde eisen voor een transactie voldoet. Er worden geen concrete gegevens uitgewisseld. Door de toepassing van homomorfe encryptie wordt de gecijferde 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.

Bevindingen

- Persoonlijk Datamanagement wordt door stakeholders gezien als een belangrijke ontwikkeling, waar het zinvol is om bij aan te sluiten. Door zich op validatie te richten en niet op gegevensverstrekking biedt TrustTester een unieke functionaliteit binnen persoonlijk datamanagement. Er is op dit moment geen andere acceptabele digitale oplossing voor het gebruik van elkaars nuttige gegevens zonder dat er profielen kunnen worden opgebouwd. (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 afhankelijk van aangesloten attribute providers; zonder deze partijen kunnen gegevens niet gevalideerd worden (k.4)⁴.
- 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).
- 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 authenticiseert 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.

⁴ De K-nummers verwijzen naar de Kwaliteitstoets in paragraaf 4.3 van het analyse rapport.

Aanbevelingen in geval brede inzet en gebruik van TrustTester binnen de overheid aan de orde is

- 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.

Het rapport van bevindingen TrustTester 1.3 kunt u downloaden van <https://www.forumstandaardisatie.nl/sites/default/files/FS/2016/1019/FS-20161019.09B-Rapport-van-bevindingen-TrustTester-1.3-0.pdf>

3. Vervolg

De resultaten van beide analyses zijn opgeleverd aan het Programma Regie op Gegevens. Op enig moment zal het Programma deze resultaten in combinatie met andere onderzoeken worden voorgelegd aan de Regieraad Dienstverlening, die over vervolg-activiteiten adviseert.