

Nota van Inlichtingen 1

Marktconsultatie Need to know en Zero trust (Kenmerk: IUC21-042)
TenderNed-kenmerk: 324613

Nr.	Datum	Positie in document	Vraag	Antwoord
1	19-08-2021	Algemeen	Wij herkennen in de marktkonsultatie de uitdaging waar de Belastingdienst voor staat. Op basis van wat wij nu weten kunnen wij, technisch gezien de uitvraag goed beantwoorden op basis van nieuwe en reeds bij de Belastingdienst in gebruik zijnde technologieën. Deze uitvraag beslaat echter vele verschillende IT aspecten zoals security, data governance over un-, semi- structured data, workflow, geolocations en meer. Doordat de uitvraag nu grotendeels gebaseerd is op een set van diverse use cases, zal een beantwoording van deze consultatie zich hier op richten. Het risico is dan dat andere, nog niet genoemde/onderkende use cases, in de toekomst net iets andere eisen aan deze oplossing zullen stellen waardoor er een miss-match ontstaat. Om beter inzicht te krijgen in de onderliggende gedachtengang en de bredere context van deze uitvraag, stellen wij voor dat de Belastingdienst samen met de geïnteresseerde leveranciers een workshop van een ongeveer dagdeel organiseert waarin deze uitvraag nader zal worden toegelicht. Bovendien geeft dat ook de ruimte tot het stellen van verdiepende vragen, resulterend in een kwalitatief beter antwoord door alle betrokkenen. Ons inziens is dit een goede aanpak om een passende, maar vooral ook toekomstvaste oplossing te kunnen garanderen.	De kern van de marktkonsultatie ziet toe op inzicht verkrijgen wat de markt kan bieden. De voorgestelde procedure bestaat uit een schriftelijke beantwoording en na selectie van een of meerdere aanbieders een POC fase. In de POC fase kan de door u voorgestelde sessie van een dagdeel plaatsvinden om zo tot een toekomstvaste oplossing te komen. Met de combinatie van de genoemde beveiligingsconcepten en het grote aantal beschreven use cases schatten wij het risico van niet onderkende situaties in als laag.
2	18-08-2021	6.3.3. P18	Kan de opdrachtgever voorbeelden geven van casussen en situaties waarbij pseudonimiseren / anonimiseren / data hiding relevant is?	Zie hiervoor hoofdstuk 8 use cases. De opdrachtgever wenst inzicht hoe u als marktpartij invulling (oplossing) zou geven aan de use cases zoals in het marktkonsultatiedocument beschreven.
3	18-08-2021	6.3.3. P18	Hoe gaat verloopt pseudonimiseren / anonimiseren / data hiding op dit moment? Wanneer gebeurt dat en door wie?	De Belastingdienst wil met marktconforme tooling en op een marktconforme wijze werken. Deze verkenning is de eerste stap. De implementatie en migratie aspecten zijn belangrijk maar zien we als onderdeel van een latere fase.

4	18-08-2021	6.3.3. P18		Om wat voor type informatie gaat het bij anonimiseren? Betreft het documenten met ongestructureerde informatie of gaat het ook om gestructureerde informatie in processen?	Vertrouwelijke informatie. Het betreft zowel ongestructureerde informatie als gestructureerde informatie.
5	18-08-2021	8 P22		Kan de opdrachtgever de casussen voor anonimiseren / pseudonimiseren en data hiding op inhoud van gegevens opnemen bij de use cases in een eventueel nieuwe versie van het document	Deze informatie is bewust niet opgenomen om ruimte te behouden voor aanbieder met een aangeboden oplossingsrichting. In de prototype fase kunnen we hier gezamenlijk een invulling voor uitwerken. Het marktconsultatie document zal daarom niet worden aangepast.
6	18-08-2021	7 P20		Opdrachtnemer ziet pseudonimiseren en anonimiseren als ander type oplossing dan autorisatie of beveiliging. De vraagstelling sluit niet geheel aan bij dit type oplossing. Kan de opdrachtgever vraagstelling rondom anonimiseren / pseudonimiseren en data hiding in de marktconsultatie opnemen bij hoofdstuk zeven?	De aanbestedende dienst begrijpt dat er een verschil is in oplossingen. Hoe dit wordt toegepast hangt af van het bestaande IT landschap en de mogelijkheden die de markt kan bieden. Deze marktconsultatie ziet toe op dat laatste. Pseudonimiseren en data hiding zien wij als een mogelijke oplossingsrichting voor use cases waarbij de gebruiker slechts een deel van de informatie mag inzien. Er zal geen aanvullende vraagstelling worden opgenomen.
7	18-08-2021	7 P21	Vraag 18	Is de opdrachtgever geïnteresseerd in een demo die zich beperkt tot het deel (automatisch) anonimiseren en pseudonimiseren (data hiding) van gegevens? Deze demo kan in een demonstratieomgeving gegeven worden en daar zijn geen verdere voorwaarden aan verbonden.	Ja. Meer informatie hierover staat in de procedurebeschrijving van het marktconsultatie document.
8	18-08-2021	7 P21	Vraag 19	Is de opdrachtgever geïnteresseerd in proof of concepts die een deel van de thematiek uit de uitvraag behandelen? Zo ja, komt automatisch anonimiseren en/of pseudonimiseren hiervoor in aanmerking?	Ja
9	200821	5.1, p. 15	nvt	In paragraaf 5.1 wordt een bestaande implementatie van RBAC processen en systemen beschreven. Is de intentie om de nieuwe oplossingen en processen te integreren met bestaande systemen en processen of worden deze geacht vervangen te worden?	Dat zou een optie kunnen zijn. Met deze verkenning zijn we benieuwd naar de mogelijkheden die de markt kan bieden.

10	200821	5.1, p. 15	nvt	In paragraaf 5.1 wordt de huidige inrichting beschreven. Er staat onder andere: "Autorisatie is op dit moment ingericht op basis van rollen." Kan de aanbestedende dienst beschrijven hoe in de huidige situatie rollen worden gekoppeld aan medewerkers?	Op basis van IMS en uitvraag van IMS in applicaties. Een verdere toelichting hierop staat in paragraaf 5.2.
11	200821	5.1, p. 15	nvt	In paragraaf 5.1 wordt de huidige inrichting beschreven. Er staat onder andere: "Autorisatie is op dit moment ingericht op basis van rollen. Medewerkers krijgen hiermee conform het RBAC beveiligingsconcept toegang tot informatie welke ze gezien hun rol mogen inzien. Deze toegang wordt geadministreerd in een centrale voorziening." a) Bedoelt de aanbestedende dienst hiermee dat voor applicaties reeds per rol is bepaald welke informatie de gebruiker mag zien conform Need to know en Zero trust? Of kan het zijn dat er in de huidige situatie nog applicaties zijn waarbij gebruikers meer informatie zien in een bepaalde rol dan volgens het principe Need to know en Zero trust wenselijk wordt geacht? b) In het verlengde: wordt in de centrale voorziening de toegang tot informatie geadministreerd, of de toegang tot bepaalde applicatiefuncties?	a) Ja, en we willen voorkomen dat een gebruiker meer kan zien dan mogelijk is. b) Beide komt voor. Indien er aanvullingen gedaan moeten worden op de centrale voorziening is dit bespreekbaar.
12	200821	5.1, p. 15	nvt	In paragraaf 5.1 wordt de huidige inrichting beschreven. Er staat onder andere: "De informatieobjecten en documenten zijn geen onderdeel zijn van het klantdossier." Kan aanbestedende dienst duiden welke informatie op dit moment wel deel uit maakt van het klantdossier?	Een klantdossier bestaat uit een combinatie van informatieobjecten en documenten. Veelal worden hier eenduidige referenties vanuit het klantdossier naar de informatieobjecten en documenten in het klantdossier opgenomen. Logisch gezien zijn ze wel onderdeel van het klantdossier.
13	200821	5.2, p. 16	nvt	In paragraaf 5.2 in het hoofdstuk over de huidige situatie wordt gesproken over VIP's en dat informatie van deze VIP's alleen door daartoe geautoriseerde gebruikers mogen worden ingezien. Kan de aanbestedende dienst beschrijven wat de definitie is van een VIP?	VIP: Very Important Person. Voor een nadere uitwerking zie paragraaf 5.2 van het marktconsultatie document.

14	200821	6.3, p. 18	nvt	Actieve monitoring is een uiterst absolute vorm van monitoring, aangezien alles dat er op een beeldscherm gebeurt, vastgelegd wordt. In welke gevallen acht u actieve monitoring noodzakelijk? Wat is de relatie tussen actieve monitoring en autorisatie en toegangscontrole?	De aanbestedende dienst wenst middels deze marktconsultatie inzage te krijgen in de oplossingsrichting die de markt kan bieden. Wanneer actieve monitoring noodzakelijk is, zal afhangen van de geboden oplossingsrichting, en is niet op voorhand bepaald.
15	200821	6.3, p. 18	nvt	In paragraaf 6.3 werd de term purpose-based credentials vermeld. Zou de aanvragende dienst kunnen verduidelijken hoe purpose-based credentials gebruikt dienen te worden?	Ons begrip van purpose-based credentials is: doel gebaseerd inloggen zien wij als een mogelijkheid om gebruikers die voor het uitvoeren van het werk extra credentials nodig hebben deze gecontroleerd toe te kennen.
16	200821	8, p. 24	nvt	Betreffende use case 15, wat wordt er bedoeld met 'extra toegang tot onderdelen van dossiers'?	Hier wordt bedoeld de situatie dat een gebruiker herhaaldelijk, onverwacht vaak, via een geautomatiseerde voorziening extra toegang tot een dossier vraagt.