

Tweede Nota van Inlichtingen (15 september 2021)

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

Nr.	Datum	Positie in document	Vraag	Antwoord
17	07-09-2021	Par. 1.2 Pag. 3	De eisen vanuit wetgeving aan de informatiebeveiliging zijn in de afgelopen jaren aangescherpt en zwaarder geworden. Welke veranderde eis(en) hebben voor de belastingdienst de meeste impact?	Op deze marktconsultatie hebben de verschillende wetten zoals opgenomen in par 4.6 van de marktconsultatie betrekking. In het bijzonder is de wetgeving en naleving betreffende de Wob, Woo en AVG de afgelopen jaren verder aangescherpt. Een combinatie van vooral deze wetten en de besluitvorming hieromtrent vanuit de politiek vormen de aanleiding voor deze marktconsultatie.
18	07-09-2021	Par. 2.2 Pag. 6	Voor uw doelstellingen hanteert de concerndirectie de standaarden en richtlijnen die vanuit Rijk en departementen zijn opgesteld en heeft deze doorvertaald. U geeft aan dat er door de concerndirectie beargumenteerd afgeweken kan worden van deze richtlijnen. Kunt u aangeven op welke punten van deze standaarden en richtlijnen binnen de Belastingdienst wordt afgeweken?	Het afwijken van standaarden en richtlijnen is situationeel. Met betrekking tot afwijkingen is geen aanvullend beleid geformuleerd.
19	07-09-2021	H. 7 Vraag 8	Een Zero Trust inrichting kent verscheidene organisatie inrichting vraagstukken en bijbehorende impact. Van welke van deze vraagstukken verwacht u het meeste risico?	Meer inzicht verkrijgen in de inrichting en de bijbehorende impact is een van de onderliggende vraagstukken waar wij middels deze marktconsultatie meer zicht op willen krijgen.
20	07-09-2021	H.7 Vraag 1	U spreekt hier over “beveiligingsconcepten...(zoals opgenomen in paragraaf 4.6.2)”? Paragraaf 4.6.2 ontbreekt echter. Met aan zekerheid grenzende waarschijnlijkheid wordt hier paragraaf 6.3 bedoeld. Kunt u dat voor de zekerheid bevestigen?	De verwijzing moet inderdaad naar Par. 6.3 zijn. De vier door ons onderkende basis beveiligingsconcepten zijn in par. 6.3 opgenomen.
21	07-09-2021	H.7 Vraag 3	Kunt u nader toelichten wat u bedoelt met “doelmatigheid”?	Met doelmatigheid wordt bedoelt: De verhouding tussen het bereiken van het resultaat en de daarvoor gebruikte menskracht en middelen.

Nr.	Datum	Positie in document		Vraag	Antwoord
22	07-09-2021	H.7 Vraag 14	Pag. 20	Wij zien bij de use cases 7 t/m 18 geen specifiek vraagstuk ontstaan op basis van de vier gedefinieerde basis beveiligingsconcepten. Wat verwacht u ten aanzien van de invulling van de use cases 7 t/m 18 en kunt u ten aanzien van deze use cases uw specifieke vraag nader formuleren?	Per use case wordt er een korte situatieschets van een probleemsituatie gegeven. Graag vernemen wij van u welke beveiligingsconcepten u voor de betreffende use case denkt in te zetten. Hierbij zien wij graag: • welk(e) beveiligingsconcept(en) word(t)(en) toegepast om het probleem op te lossen; • op welke wijze het betreffende beveiligingsconcept wordt ingezet; • wat de organisatorische en technologische impact is op de Belastingdienst organisatie en IT-landschap; • op welke wijze wij de voorgestelde oplossing kan worden ingericht (praktische invulling).
23	08-09-2021	Par. 4.2	Pag. 12	Is Customer Identity Management (m.b.t. de belastingbetaler) in scope voor toekomstige werkzaamheden en/of projecten?	Customer identity management an sich valt buiten de scope van deze marktkonsultatie. Deze marktkonsultatie ziet toe op toegang tot informatie zoals dossiers. De toegang tot informatie is afhankelijk van de toegekende rechten. Het komt voor dat ten aanzien van hetzelfde dossier de behandelaar en de belastingbetaler deels toegang verkrijgen tot dezelfde informatie, en deels toegang verkrijgen tot andere delen van de informatie (zie use case 8). Wij zijn benieuwd op welke manier dit op een doelmatige manier ingericht kan worden.
24	08-09-2021	Par. 5.1	Pag. 15	In relatie tot Customer Identity Management: op dit moment verzorgen DigiD en e-Herkenning identity autorisatie voor belastingbetalers. Bevatten deze kanalen extra risico's?	Voor deze marktkonsultatie is dit niet van toepassing. Voor zover deze kanalen risico's bevatten vallen deze buiten scope en de beantwoording van deze marktkonsultatie.

Nr.	Datum	Positie in document		Vraag	Antwoord
25	08-09-2021	Par. 5.1	Pag. 15	In relatie tot DigiD: heeft de Belastingdienst contact gehad met Logius over het onderwerp en de scope van de marktconsultatie?	Nee, er is voorafgaand aan deze marktconsultatie hieromtrent geen contact geweest met Logius. Reden hiervoor is dat de toepassing van DigiD buiten de scope van deze marktconsultatie valt.
26	08-09-2021	Par. 5.1	Pag. 15	Heeft de Belastingdienst een datamanagementprogramma lopen toegespitst op het onderwerp en de scope van de marktconsultatie?	Ja. Binnen de Belastingdienst loopt er een datamanagementprogramma. De inrichting van beveiligingsconcepten wordt gezien als randvoorwaardelijk voor de inrichting van het datamanagementprogramma.

Eerste Nota van Inlichtingen (27 augustus 2021)

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 marktconsultatie 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 marktconsultatie 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.

Nr.	Datum	Positie in document		Vraag	Antwoord
2	18-08-2021	6.3.3	Pag. 18	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 marktconsultatiedocument beschreven.
3	18-08-2021	Par. 6.3.3	Pag. 18	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	Par. 6.3.3	Pag. 18	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	H. 8	Pag. 22	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	H. 7	Pag. 20	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.

Nr.	Datum	Positie in document		Vraag	Antwoord
7	18-08-2021	H. 7 Vraag 18	Pag. 21	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	H. 7 Vraag 19	Pag. 21	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	21-08-2021	Par. 5.1	Pag. 15	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	21-08-2021	Par. 5.1	Pag. 15	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.

Nr.	Datum	Positie in document		Vraag	Antwoord
11	21-08-2021	Par. 5.1	Pag. 15	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	21-08-2021	Par. 5.1	Pag. 15	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	21-08-2021	Par. 5.2	Pag. 16	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.

Nr.	Datum	Positie in document		Vraag	Antwoord
14	21-08-2021	Par. 6.3	Pag. 18	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	21-08-2021	Par. 6.3	Pag. 18	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	21-08-2021	H. 8 Use case 15	Pag. 24	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.