



Belastingdienst

Marktconsultatie

Need to know en Zero trust

Aanbestedende dienst(en):

- Inkoop uitvoeringscentrum Belastingdienst

Versie : 1.0 Definitief
Kenmerk : IUC21-042
Datum : 06 augustus 2021

Inhoud

Hoofdstuk 1.	Algemeen	3
1.1	Leeswijzer	3
1.2	Inleiding.....	3
1.3	Hoofdvraag Marktconsultatie.....	3
Hoofdstuk 2.	De Belastingdienst	5
2.1	Organisatie van de Belastingdienst	5
2.1.1	Primaire-procesdirecties:.....	5
2.1.2	Concerndirecties	5
2.1.3	Corporate diensten en Shared Service Organisaties	5
2.2	Concerndirectie IV- en Databeheersing.....	6
Hoofdstuk 3.	Procedure	7
3.1	Algemeen	7
3.2	Inkoop Uitvoeringscentrum (IUC) Belastingdienst	7
3.3	Contact.....	7
3.4	Planning	8
3.5	Marktconsultatiedocument.....	8
3.6	Toelichting en aanvullende vragen (optioneel)	9
3.7	Best practices, patronen en demonstratie	9
3.8	Proof of concept	9
3.9	Vormvereisten	10
3.10	Randvoorwaarden deelname aan deze marktconsultatie	10
Hoofdstuk 4.	Context en kaders	12
4.1	Hoofddoelstellingen Belastingdienst.....	12
4.2	Hoofgebieden	12
4.3	Algemene architectuur kaders.....	13
4.4	Regelgeving rondom informatiebeveiliging	13
4.5	Kaders	14
4.6	Vigerende wetgeving	14
Hoofdstuk 5.	Huidige situatie	15
5.1	Huidige inrichting	15
5.2	Afscherming gegevens	16
Hoofdstuk 6.	Gewenste situatie	17
6.1	Gewenste omgeving.....	17
6.2	Informatiebeveiliging.....	17
6.3	Need to know en Zero trust.	17
6.4	Uitgangspunt voor de werkplek van de medewerker.	18
6.5	De compliance werkomgeving.....	18
6.6	Informatie uitwisseling met belastingplichtigen.....	19
6.7	Inrichting vertrouwelijkheidsservice bij de werkomgeving van de medewerker.....	19
Hoofdstuk 7.	Vragen	20
Hoofdstuk 8.	Use cases	22

Hoofdstuk 1. Algemeen

1.1 Leeswijzer

In dit hoofdstuk wordt kort de aanleiding voor de marktconsultatie beschreven. Hoofdstuk 2 beschrijft de organisatie van de Belastingdienst en de betrokken onderdelen, in hoofdstuk 3 wordt de te volgen marktconsultatieprocedure beschreven. Hoofdstuk 4 geeft inzicht in de van toepassing zijnde context en kaders. In hoofdstuk 5 en 6 worden respectievelijk de huidige en gewenste situatie beschreven, waarna in hoofdstuk 7 de vragen worden gesteld. Ten slotte worden in hoofdstuk 8 de onderkende use cases beschreven.

1.2 Inleiding

De eisen vanuit wetgeving aan de informatiebeveiliging zijn in de afgelopen jaren aangescherpt en zwaarder geworden. De publieke opinie over het beschikbaar stellen en gebruiken van informatie bij het uitvoeren van taken is aan het veranderen. Hiernaast en hierdoor is er ook vanuit de politiek meer aandacht/toezicht voor juist gebruik van informatie.

De Belastingdienst, Douane en Toeslagen willen in de veranderende omgeving rondom informatiebeveiliging de medewerkers een werkplek bieden die is toegerust op de medewerker en waarbij de toegang tot informatie conform de wetgeving is ingericht en hij of zij zich daarover dan ook geen zorgen meer hoeft te maken. Conform het **Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013** (VIRBI 2013) hebben we hierbij als uitgangspunt dat een medewerker zoveel toegang en autorisatie tot systemen en gegevens heeft als nodig, en ook niet meer.

Onder regie van het Inkoop Uitvoeringscentrum (IUC) Belastingdienst voert de Concerndirectie IV&D mede namens Douane en Toeslagen deze marktconsultatie uit.

Voor alle duidelijkheid: het betreft hier GEEN offerteaanvraag en deze marktconsultatie dient uitdrukkelijk niet om een voorselectie te maken van marktpartijen in het kader van een mogelijke toekomstige aanbesteding.

1.3 Hoofdvraag Marktconsultatie

IV&D heeft behoefte aan een nadere uitwerking van het Need-to-know en Zero trust principe. Met deze marktconsultatie wil IV&D onderzoeken welke oplossingsconcepten de markt heeft ontwikkeld, op welke wijze die binnen de omgeving van de Belastingdienst uitvoerend kunnen worden ondersteund al dan niet met behulp van tooling c.q. product en welk volwassenheidsniveau is bereikt.

De resultaten van de marktconsultatie zijn voor de Belastingdienst input voor het opstellen van beleid, enterprise- en domeinarchitectuur en een mogelijk toekomstige aanbesteding. Tevens willen wij een indicatie krijgen van de kosten en de kostenelementen van de voorgestelde oplossing.

De Belastingdienst heeft uiteindelijk behoefte aan een oplossing welke ingezet kan worden ten behoeve van de volgende hoofdgebieden:

- Interactie;
- Toezicht;
- Massale transactieverwerking:
 - gegevensdiensten;
 - heffing en toekennen;
 - Inning en uitbetalen;
- Sturen & Verantwoorden;
- Bedrijfsvoering.

Deze hoofdgebieden zijn beschreven in de Belastingdienst concernarchitectuur.

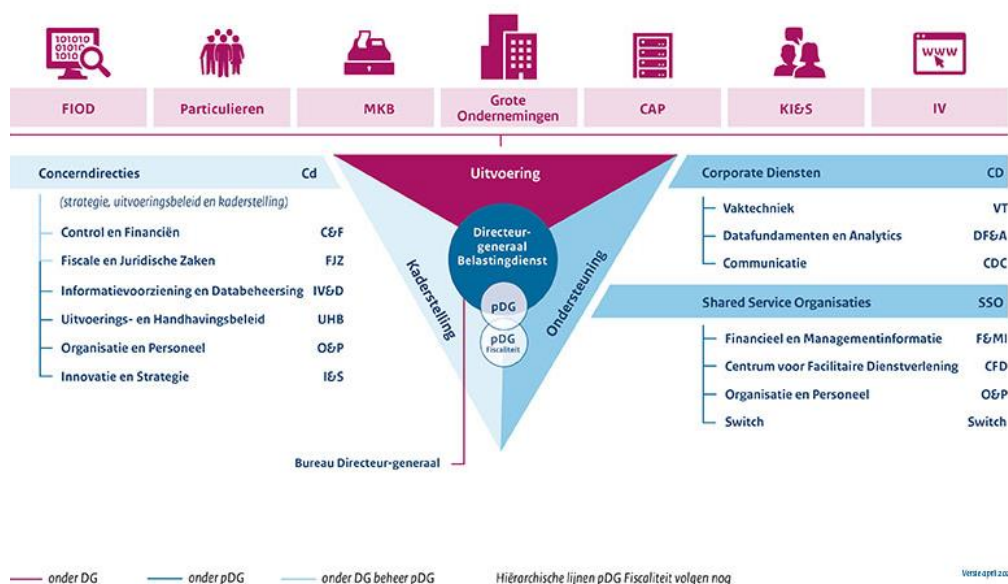
Hoofdstuk 2. De Belastingdienst

De Belastingdienst valt onder het ministerie van Financiën. Door de ontvlechting maken Toeslagen en Douane geen onderdeel meer uit van de Belastingdienst. Dit zijn nu zelfstandige onderdelen van het ministerie van Financiën. Bij de Belastingdienst werken nu bijna 25.000 mensen. Een groot deel van de medewerkers heeft direct contact met burgers en bedrijven. De rest van de medewerkers werkt bij de facilitaire bedrijven, conserndirecties en corporate diensten binnen de Belastingdienst.

2.1 Organisatie van de Belastingdienst

De Belastingdienst kent drie soorten directies

- Uitvoerende taken door de Primaire-procesdirecties;
- Strategie, kaders en uitvoeringsbeleid door de Conserndirecties;
- Ondersteunende taken door de Corporate diensten en Shared Service Organisaties.



Figuur 1. Organogram Belastingdienst

2.1.1 Primaire-procesdirecties:

Deze directies voeren elke dag de kerntaken van de Belastingdienst uit, zoals belastingen innen en toeslagen uitkeren. Deze uitvoerende taken zijn belegd bij negen directies: Particulieren, Midden- en Kleinbedrijf, Grote Ondernemingen, Fiscale Inlichtingen- en Opsporingsdienst (FIOD), Centrale Administratieve Processen, Klantinteractie en Services en Informatievoorziening. Deze directies worden direct aangestuurd door de directeur-generaal Belastingdienst.

2.1.2 Conserndirecties

Deze directies zijn verantwoordelijk voor de kwaliteit, kaders en het uitvoeringsbeleid. Zij worden aangestuurd door de plaatsvervangend directeur-generaal.

2.1.3 Corporate diensten en Shared Service Organisaties

Deze directies voeren ondersteunende taken uit. Zij worden aangestuurd door de plaatsvervangend directeur-generaal.

2.2 Concerndirectie IV- en Databeheersing

Het is de missie van IV&D om zeker te stellen dat de informatievoorziening (IV) voor de kerntaken van de Belastingdienst (heffen, innen, uitkeren, goederentoezicht en opsporing) zich beheerst blijft vernieuwen in lijn met de ambities van het ministerie van Financiën en de Belastingdienst. Voor de informatievoorziening (IV) richten zij zich op het borgen van de continuïteit, het verhogen van de adaptiviteit, voorspelbaarheid, productiviteit, betrouwbaarheid, het garanderen van een veilige omgang met gegevens en borging van de privacy.

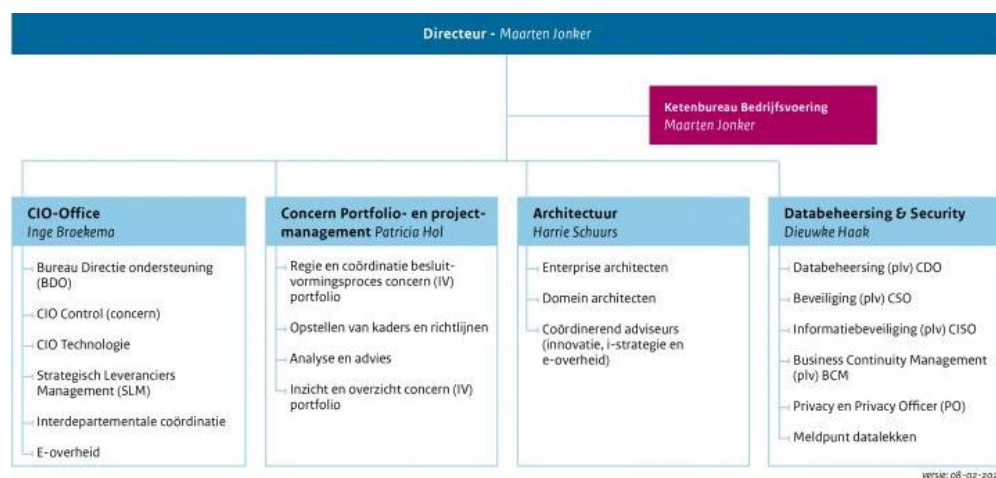
De Concerndirectie IV&D verbindt de Belastingdienst aan het rijksbeleid voor de informatievoorziening. Daarvoor onderhouden zij afstemming met het kerndepartement en verzorgen zij kaderstelling voor het concern.

Het is de hoofddoelstelling van de Concerndirectie IV&D om de kerntaken van de Belastingdienst met kaderstellend beleid en opvolging daarvan te ondersteunen.

Daarbij staan de volgende doelen centraal:

Continuïteit	Het behouden en waar nodig verhogen van de continuïteit en beschikbaarheid van de informatievoorziening, de fysieke beveiliging en de bedrijfscontinuïteit.
Adaptiviteit	Het omvormen van het huidige statische IV-landschap naar een informatievoorziening die adaptief is ten opzichte van nieuwe (wettelijke) eisen en technologische mogelijkheden.
Voorspelbaarheid	Het richten (beleid), inrichten (kaders) en regie nemen op lijn, project-, portfolio- en risicomanagement ⁸ van IV vanuit strategie en noodzaak (business rationale), maakbaarheid (architectuur), haalbaarheid (budget/resources) en risico's.
Betrouwbaarheid	Het bevorderen van een juiste omgang met (persoons)gegevens (AVG, AWR, AWIR en WPG), actuele informatiebeveiliging en weerbaarheid tegen cybercriminaliteit.
Productiviteit	Het verhogen van de efficiency van informatievoorziening, het faciliteren van strategische investeringsbeslissingen, functioneel sturen op efficiënte, effectieve en voorspelbare IV-voortbrengingsketens en tijdig onderhoud en technologisch vernieuwing.

Hierbij hanteert de concerndirectie de standaarden en richtlijnen die vanuit Rijk en departementen zijn opgesteld en vertaalt zij deze door. Waar dit vanuit de specifieke eisen van de Belastingdienst noodzakelijk is, kan hier beargumenteerd van worden afgeweken.



Figuur 2. Organogram IV&D

Hoofdstuk 3. Procedure

3.1 Algemeen

Iedere belangstellende marktpartij mag deelnemen aan deze marktconsultatie. Aan de deelnemers aan deze marktconsultatie wordt gevraagd de in hoofdstuk 5 gestelde vragen te beantwoorden.

Het indienen van schriftelijke reacties kan via TenderNed. Wij ontvangen uw bijdrage aan de marktconsultatie graag zo spoedig mogelijk maar uiterlijk op maandag 20 september 2021, via de berichtenmodule van TenderNed.

3.2 Inkoop Uitvoeringscentrum (IUC) Belastingdienst

Inkoop Uitvoeringscentrum Belastingdienst (IUC Belastingdienst) is onderdeel van Shared Service Organisatie Centrum voor Facilitaire Dienstverlening (SSO CFD) en is de dienst die namens de Belastingdienst aanbestedingen uitvoert. In het kader van een compacte rijksdienst is IUC Belastingdienst per 1 januari 2013 een Inkoop Uitvoeringscentrum (IUC) voor de Rijksoverheid. Dit betekent een uitbreiding van taken en opdrachtgevers buiten de Belastingdienst. IUC Belastingdienst verricht inkoopactiviteiten voor de generieke inkoop van de bij hem ondergebrachte rijks categorieën en daarnaast voor de specifieke inkoop van de Belastingdienst en Domeinen Roerende Zaken. Hij doet dat op een wijze die effectief, doelmatig, transparant en rechtmatig is.

3.3 Contact

De Belastingdienst hanteert voor deze marktconsultatie heldere regels, daarom dient u alleen met onderstaande contactpersoon over deze marktconsultatie te communiceren via TenderNed. Communiceert u over deze marktconsultatie met andere medewerkers van de Belastingdienst of tracht u via andere kanalen hen te beïnvloeden dan kan dat een reden zijn voor de Belastingdienst om u uit te sluiten van verdere deelname aan deze marktconsultatie.

Contactpersoon	
Naam:	J. (Jaques) Heeren
Functie:	Inkoopspecialist ICT
E-mail:	j.heeren@belastingdienst.nl

Tabel 1. Contactpersoon

3.4

Planning

Hieronder wordt de planning van deze marktconsultatie weergegeven. De planning is indicatief, waaraan geen rechten kunnen worden ontleend.

Activiteit	Datum
Fase: Marktconsultatie	
Publicatie marktconsultatie op TenderNed	vr. 06 aug. 2021
Uiterste datum voor het stellen van vragen voor de eerste vragenronde	vr. 20 aug. 2021
Publicatie eerste nota van inlichtingen	vr. 27 aug 2021
Uiterste datum voor het stellen van vragen voor de tweede vragenronde	wo. 08 sept 2021
Publicatie tweede nota van inlichtingen	wo. 15 sept. 2021
Uiterst moment van insturen reactie.	ma. 20 sept. 2021; 12:00 uur
Toelichting en aanvullende vragen	vr. 24 sept. 2021
Fase: Productdemonstratie	
Partijen uitnodiging voor demonstratie	vr. 01 okt 2021
Uitvoeren van productdemonstraties	ma. 11 okt. t/m vr. 15 okt. 2021
Fase: Proof of concept	
Partijen uitnodigen voor proof of concept	vr. 22 okt. 2021
Afstemmen en voorbereiden proof of concept	ma. 25 okt. t/m vr. 12 nov. 2021
Uitvoeren proof of concept	ma. 15 nov. t/m vr. 17 dec 2021

Tabel 2. Planning

De Belastingdienst maakt u erop attent dat de datum en tijd zoals vermeld op de website van TenderNed leidend is. De vermelde tijden zijn tijden in de tijdzone zoals in Nederland van toepassing (Central European Time).

3.5

Marktconsultatiedocument

Op basis van het voorliggende document kunnen marktpartijen een reactie geven op de in deze marktconsultatie gestelde vragen. De Belastingdienst heeft hiertoe in dit document de behoefte omschreven en toegelicht volgens welke procedure deze marktconsultatie verloopt.

Ten aanzien van nadere inlichtingen of vragen over de marktconsultatie, wordt u verzocht deze zo spoedig mogelijk via een bericht op TenderNed kenbaar te maken. Wij verzoeken u hiervoor gebruik te maken van het document “Vragen tbv Nota van Inlichtingen”. Vragen dienen uiterlijk op de bij ‘Termijnen’ in TenderNed opgenomen datum en tijdstip via TenderNed ingediend te worden.

De Belastingdienst beantwoordt alle vragen geanonimiseerd. De vragen en antwoorden zijn na de publicatie tegelijkertijd voor alle geïnteresseerde marktpartijen op TenderNed beschikbaar. Eventuele aanvullingen en correcties op het marktconsultatiedocument wordt tevens via TenderNed gepubliceerd.

De resultaten van deze marktconsultatie kunnen worden verwerkt in Belastingdienst beleidsdocumenten, Belastingdienst enterprise- en domeinarchitectuur, aanbestedingsdocumenten en/of openbaar gemaakt, zonder dat deze herleidbaar zijn tot de deelnemers van de marktconsultatie. De Belastingdienst mag vrij over de verstrekte informatie beschikken en deze informatie gebruiken. Wij verzoeken u de vragen schriftelijk te beantwoorden. De door u gegeven informatie zal vertrouwelijk worden behandeld.

Mogelijk wordt u benaderd om uw product te presenteren tijdens een productdemonstratie met vertegenwoordigers van de Belastingdienst als ook om deel te nemen aan een proof of concept.

3.6 Toelichting en aanvullende vragen (optioneel)

De Belastingdienst zal mogelijkerwijs naar aanleiding van de ontvangen reacties aan deelnemers aan deze marktconsultatie vragen de antwoorden nader toe te lichten of aanvullende vragen te beantwoorden.

3.7 Best practices, patronen en demonstratie

De Belastingdienst heeft het voornemen om enkele partijen (de Belastingdienst streeft naar een maximum aantal van zes partijen) uit te nodigen voor een algemene demonstratie van de voorgestelde oplossing. Doel van deze demonstratie is:

- inzicht krijgen in de algemene werking van best practices en geadviseerde patronen;
- Inzicht krijgen in de algemene werking van de voorgestelde oplossing;
- inzicht krijgen in de toepasbaarheid en integratie van de best practice, geadviseerde patronen en voorgestelde oplossing binnen de Belastingdienst(omgeving).

De Belastingdienst heeft de voorkeur dat de producent van het desbetreffende product welke gebruikt worden binnen de voorgestelde oplossing (eventueel in samenwerking met een integratiepartner) de demonstratie uitvoert. Indien een product door meerdere deelnemende marktpartijen wordt voorgesteld wordt getracht om per product maximaal één demonstratie uit te laten voeren.

3.8 Proof of concept

In aanvulling op de algemene demonstratie van de voorgestelde oplossing is de Belastingdienst voornemens om met een klein aantal partijen (streven is een maximum aantal van drie) uit te nodigen voor een meer diepgaande proof of concept. De Belastingdienst wil dit in de periode van 15 november 2021 tot en met 17 december laten plaatsvinden.

Tijdens deze proof of concept zullen aan de hand van diverse Belastingdienst specifieke use cases in de door de marktpartij voorgestelde oplossing worden getest. Hier willen we uitgebreid aandacht besteden aan de organisatorische inrichting en het benoemen van de consequenties voor de uitvoeringsorganisatie.

De proof of concept zal op een omgeving (van de deelnemende marktpartij) uitgevoerd worden welke vergelijkbare relevante kenmerken bezit (de invulling hiervan zal gezamenlijk afgestemd worden). Hierbij zullen diverse specifieke use cases (gebaseerd op de use cases zoals beschreven in hoofdstuk 6) behandeld worden. De Belastingdienst heeft de voorkeur om met de producenten van het desbetreffende product (eventueel in samenwerking met een integratiepartner) de proof of concept uit te voeren. Indien een product door meerdere deelnemende marktpartijen wordt voorgesteld wordt getracht om per product maximaal één proof of concept uit te laten voeren.

Doel van de proof of concept is zicht krijgen op:

- De inzet van de voorgestelde oplossing in relatie tot de specifieke Belastingdienst problemen en de mate waarin de genoemde doelstellingen gerealiseerd kunnen worden;
- de toepasbaarheid en bruikbaarheid van de voorgestelde oplossing binnen de specifieke Belastingdienst omgeving;
- hoe de voorgestelde oplossing invulling kan geven binnen een Need to know architectuur by design;
- een blauwdruk voor inrichting van de Business en IV-organisatie om de voorgestelde oplossing optimaal te kunnen inzetten;
- consequenties voor beheer (waaronder gebruiksrechten);
- consequenties voor de uitvoeringsorganisatie (dagelijks gebruik door eindgebruiker);
- de implementatiewerkzaamheden, -doorlooptijd en -inspanning (incl. inrichting, parameterisering, opleiding en certificering).

We verzoeken u in uw reactie op de marktconsultatie aan te geven of u bereid bent mee te werken aan een op de Belastingdienst toegesneden demonstratie en uitgebreide proof of concept. Wij zijn bereid om een deel van de uren voor de uitvoering van de proof of concept te vergoeden. Hiervoor is een maximum vergoeding per deelnemende marktpartij van € 15.000 beschikbaar. De maximale vergoeding is gebaseerd op 20 werkdagen á € 750 per dag. Als u gebruik wenst te maken van deze vergoeding dan wordt u verzocht dit in uw reactie bij vraag 18 (hoofdstuk 7, inclusief een onderbouwing van de uren) kenbaar te maken. Voorafgaand aan de proof of concept zullen hier afspraken over gemaakt worden. Als u er (aanvullende) voorwaarden verbonden zijn aan de demonstratie en/of de proof of concept dan dient u dit in uw reactie duidelijk te vermelden bij de vragen 17 en 18 (hoofdstuk 7).

3.9 Vormvereisten

Het is uitdrukkelijk niet de bedoeling offertes in te leveren, wij verzoeken u dringend om u te beperken tot de beantwoording van de gestelde vragen in Hoofdstuk 5. Beantwoording graag kort en krachtig. Uiteraard bent u niet verplicht tot het verstrekken van antwoorden en u bent eveneens vrij bepaalde vragen over te slaan. De bijdrage aan de marktconsultatie/beantwoording van de vragen ontvangen wij bij voorkeur in Word of Excel format. Aanvullende en overige documentatie mogen ook als pdf-bestand worden aangeleverd.

In de begeleidende brief bij uw reactie op de marktconsultatie ontvangen wij graag van de contactpersoon aan de kant van de deelnemende marktpartij de onderstaande gegevens:

- Naam;
- Functie;
- Kantooradres;
- Telefoonnummer;
- E-mail adres.

3.10 Randvoorwaarden deelname aan deze marktconsultatie

Door deelname aan deze marktconsultatie gaat u onvoorwaardelijk akkoord met de alle voorwaarden zoals vermeld in dit marktconsultatiedocument. Hieronder staan de randvoorwaarden limitatief opgesomd:

Deelnemen aan de marktconsultatie is voor marktpartijen én de Belastingdienst vrijblijvend;

1. Dit marktconsultatiedocument is uitsluitend bestemd voor marktconsultatie doeleinden;
2. De marktconsultatie is geen onderdeel van een mogelijke aanbesteding maar een consultatieronde;

3. Door de deelnemers aan deze marktconsultatie kunnen geen kosten in rekening worden gebracht aan de Belastingdienst in verband met het uitbrengen van de reactie op deze marktconsultatie en de daarvoor uit te voeren werkzaamheden (met uitzondering van de vergoeding voor de proof of concept);
4. Deze marktconsultatie dient uitdrukkelijk niet om een voorselectie te maken van marktpartijen in het kader van een mogelijke toekomstige aanbesteding. Marktpartijen die niet deelnemen aan de marktconsultatie zijn daarmee niet uitgesloten van deelname aan een mogelijk inkooptraject. Evenmin zijn marktpartijen die deelnemen aan de marktconsultatie op enige wijze uitgesloten van, of bevoorrecht in, een eventuele deelname aan een aanbestedings- of inkooptraject;
5. De resultaten van de marktconsultatie worden mogelijk verwerkt in documenten voor beleid, enterprise- en domeinarchitectuur en aanbestedingsdocumenten (bijvoorbeeld door tijdens deze marktconsultatie ontvangen informatie te verwerken in het Beschrijvend document), zonder dat deze herleidbaar zijn tot de deelnemers aan de marktconsultatie. Door deel te nemen aan marktconsultatie stemt u hiermee in;
6. Verstreckte informatie in het kader van de marktconsultatie kan afwijken van in de aanbestedingsprocedure te verstrekken informatie;
7. De inbreng van deelnemers aan deze marktconsultatie zal zoveel mogelijk vertrouwelijk behandeld worden, waarbij in ieder geval rekening zal worden gehouden met de gerechtvaardigde belangen van de deelnemers van deze marktconsultatie en de Belastingdienst;
8. De voertaal tijdens deze marktconsultatie is Nederlands, algemene productinformatie mag in het Engels;
9. De Belastingdienst is op geen enkele wijze gebonden aan de uitkomsten van de marktconsultatie;
10. Deelnemers aan de marktconsultatie kunnen geen rechten ontleen aan deelname aan de marktconsultatie of aan enige informatie die tijdens de marktconsultatie wordt verstrekt;
11. Het accepteren of honoreren van eventuele voorwaarden of claims (waaronder voorwaarden of claims t.a.v. Intellectuele Eigendomsrechten zoals auteursrecht) van deelnemers aan deze marktconsultatie over het gebruik van door hen aan de Belastingdienst in het kader van deze marktconsultatie informatie of vertrouwelijkheid en geheimhouding van door de betreffende marktpartij verstreckte informatie is niet mogelijk. Wel zal de Belastingdienst bij het verstrekken, openbaren of verwerken van informatie verkregen van deelnemers tijdens, of voortvloeiend uit, deze marktconsultatie zoveel mogelijk trachten te voorkomen dat deze informatie direct herleidbaar is tot een bepaalde deelnemer van de marktconsultatie.
12. Indien intellectuele eigendomsrechten (waaronder auteursrechten) van een deelnemer of van derden van toepassing zijn dan wordt de Belastingdienst door de betreffende deelnemer aan deze marktconsultatie gevrijwaard van een vordering van deze deelnemer en/of derden op basis van die intellectuele eigendomsrechten (waaronder auteursrechten).
13. De Belastingdienst behoudt zich het uitdrukkelijk het recht voor de planning van deze marktconsultatie zoals opgenomen in dit document te wijzigen. Daarnaast ook om de marktconsultatie tijdelijk en/of definitief te staken.

Hoofdstuk 4. Context en kaders

4.1 Hoofddoelstellingen Belastingdienst

De Belastingdienst werkt conform onderstaande hoofddoelstellingen. Verdere invoering van Need to know en Zero trust beveiligingsconcepten moet de realisatie van deze hoofddoelstellingen ondersteunen.

Hoofddoelstellingen	Verbeterdoelen
Snelle, betrouwbare en zorgvuldige behandeling	De Belastingdienst werkt informatie gestuurd, doelgroepgericht en in de actualiteit. Hij gaat veilig om met de gegevens die hij voor de uitvoering van zijn taak nodig heeft. Hij streeft ernaar het burgers en bedrijven gemakkelijk te maken om aan hun verplichtingen te voldoen en fouten te voorkomen, bijvoorbeeld door het vooraf invullen van informatie in aangiften. Burgers en Bedrijven kunnen op ieder moment een overzicht van hun fiscale situatie inzien en digitaal hun belastingzaken regelen
Deskundige en persoonlijke ondersteuning waar nodig	Dienstverlening is een onlosmakelijk onderdeel van ons werk. Onze dienstverlening is proactief en we verliezen de menselijke maat niet uit het oog. Waar burgers en bedrijven onvoldoende geholpen zijn met de massale voorzieningen bieden we persoonlijke hulp. We werken samen met publieke en private partners en maken het mogelijk dat burgers en bedrijven hun fiscale zaken door een adviseur laten afhandelen. We streven ernaar vragen en problemen zo goed mogelijk in één keer op te lossen.
Effectief toezicht en fraudebestrijding	We bevorderen de naleving door proactief en in de actualiteit te handelen en fouten te voorkomen. Waar mogelijk voeren we toezicht vooraf uit, waar nodig achteraf. We gebruiken daarbij data-analyse en borgen dat we voldoen aan de eisen op het gebied van rechtsstatelijkheid, privacy en non-discriminatie. We stemmen de middelen die we inzetten af op het gedrag en de houding van burgers en bedrijven en hebben oog voor situaties waarbij schade op kan treden voor burgers en bedrijven als we binnen de wet- en regelgeving onvoldoende rekening houden met hun situatie.
Wendbare en toekomstbestendige organisatie	We brengen focus aan op concrete doelen en maken keuzes. We anticiperen op veranderingen in het maatschappelijk veld. Het invullen van randvoorwaarden op het gebied van personeel, cultuur, ICT, gegevens en sturing & beheersing heeft onze permanente aandacht.

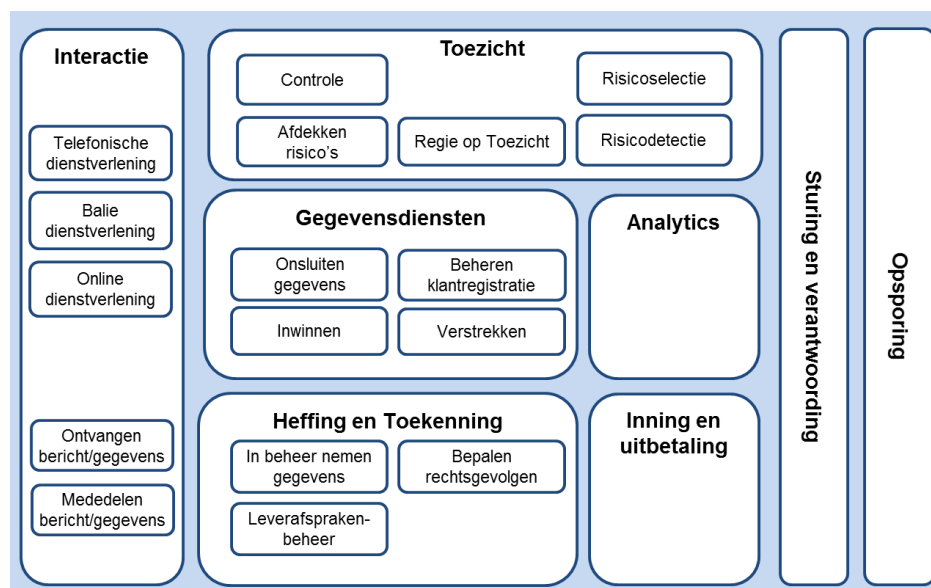
Tabel 3. Belastingdienst hoofddoelstellingen

4.2 Hoofgebieden

De beschrijving van de huidige situatie van Need to know en Zero trust heeft betrekking op de onderstaande hoofdgebieden. Deze hoofdgebieden zijn tevens de scope voor de gewenste situatie.

- Interactie;
- Toezicht;
- Massale transactieverwerking:
 - Gegevensdiensten;
 - heffing en toekennen;
 - Inning en uitbetalen;
- Sturen & Verantwoorden;
- Bedrijfsvoering.

De hoofdgebieden zijn beschreven in de Belastingdienst concernarchitectuur.



Figuur 3. Belastingdienst Capability model

4.3 Algemene architectuur kaders

De Belastingdienst hanteert diverse kaders bij de vormgeving van haar informatievoorziening, waarvan de belangrijkste zijn:

- Lijst van open IT-standaarden zoals vastgesteld door het forum standaardisatie: Zie: <https://www.forumstandaardisatie.nl/node/217>.
- Architectuurprincipes zoals vastgelegd in de Nederlandse Overheid Referentie Architectuur (NORA). De principes van de NORA zijn bedoeld om overheidsorganisaties richting te duiden bij het inzetten van veranderingen en het uitvoeren van projecten. De principes zijn beschreven in relatie tot relevante beleidskaders, vastgestelde standaarden, reeds beschikbare bouwstenen en voorbeelden, opdat de herkenbaarheid met de praktijk zo groot mogelijk is. <https://www.noraonline.nl/wiki/Principes>

4.4 Regelgeving rondom informatiebeveiliging

De Belastingdienst moet voor het aandachtgebied Need to know voldoen aan de relevante regelgeving. De belangrijkste onderdelen hiervan zijn:

- De **Baseline informatiebeveiliging Overheid (BIO)**, **VIR2007**, **VIRBI2013** en **AVG** zijn het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen.
- Kaders omtrent het gebruik van gemeenschappelijke voorzieningen van de **digitale overheid** (bijv. DigiD en basisregistraties).

Het is belangrijk dat de oplossing past binnen de architectuur kaders en regelgeving. Vanzelfsprekend is daarnaast van belang dat voldaan kan worden aan alle relevante wet en regelgeving, zie hiervoor onderstaande paragrafen: 4.5 Kaders en 4.6 Vigerende wetgeving.

4.5 Kaders

De Belastingdienst moet voor het aandachtgebied Need to know voldoen aan de relevante kaderstelling De belangrijkste onderdelen hiervan zijn:

- | | |
|------------|---|
| BIO en iBB | <p>Baseline Informatiebeveiliging Overheid en
 Integraal Beveiligingsbeleid Belastingdienst (niet openbaar).</p> <p>Eisen vanuit aantoonbaarheid van handelen:
 Alle handelingen die worden uitgevoerd zijn onweerlegbaar herleidbaar tot (de verantwoordelijkheid van) een natuurlijk persoon. Zoals beschreven in het iBB (paragraaf 3.2.2 punt b).</p> <p>Uit het iBB Paragraaf 3.2.2 punt b. We beschermen geclassificeerde bedrijfsmiddelen.
 De beleidsuitgangspunten zijn hierbij:</p> <ul style="list-style-type: none"> • De veiligheid van medewerkers, bezoekers en leveranciers binnen de eigen gebouwen en terreinen staat voorop. • Toegang en autorisatie wordt verleend op basis van Need-to-know, Need-to-do en het principe van least privilege
 least privilege: alleen de autorisaties die iemand nodig heeft om zijn taak te kunnen vervullen, zullen worden toegekend (sic), conform VIRBI 2013). |
|------------|---|

4.6 Vigerende wetgeving

De Belastingdienst moet voor het aandachtgebied Need to know voldoen aan de wetgeving. De belangrijkste onderdelen hiervan zijn:

- | | |
|-----|--|
| AVG | <p>Algemene Verordening Gegevensbescherming
 Privacywetgeving; juiste autorisatie zodat de informatie toegankelijk is alleen waar dit nodig is (Need to know)</p> |
| AW | <p>ArchiefWet
 Bewaartermijnen worden nageleefd</p> |
| Wob | <p>Wet openbaarheid van bestuur
 Verschaft inzage in het handelen van de overheid</p> |
| Woo | <p>Wet open overheid
 Als de Woo van kracht wordt, vervangt deze wet de Wob
 Informatie is (pro actief) snel en volledig beschikbaar</p> |
| AWR | <p>Algemene Wet Rijksbelastingen
 Een dossier van een burger/bedrijf is tijdig, volledig en juist (kwaliteit)</p> |
| WAU | <p>Rapport Werk Aan Uitvoeren
 Het is transparant hoe processen lopen (track & trace)</p> |

Hoofdstuk 5. Huidige situatie

De bestaande oudere Belastingdienst IV-voorzieningen ondersteunen onvoldoende 'by design' Need to Know. Daar waar Need to know als beveiligingsconcept is geïmplementeerd is dat op basis van het Roll Based Access Control (RBAC).

In de onderstaande paragrafen is de huidige inrichting nader uitgewerkt.

5.1 Huidige inrichting

De bestaande implementatie van identificatie en authenticatie is ingericht op basis van gebruikersnaam-wachtwoord gekoppeld aan het gebruikte device. 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.

De IAM inrichting voorziet in het beperken van wat een medewerker mag doen in een bepaalde applicatie. Welke informatie de medewerker mag (in)zien wordt door het ontwerp van de applicatie (by design) beperkt. De geldigheid in tijd en geldigheidsduur van rechten op dossiers is nu niet ingericht. De medewerker heeft op basis van zijn ID toegang tot een persoonlijke mail en de documentmanagement omgeving.

Conform de Need to Know uitgangspunten is meer informatie beschikbaar dan voor het uitvoeren van het werk op dat moment noodzakelijk is. De inrichting van Need to know is in deze situatie gebaseerd op het vertrouwen wat de Belastingdienst in de medewerkers stelt. Om alle informatie van een subject te bepalen moeten naast de gemeenschappelijke dataomgevingen meerdere systemen geraadpleegd worden. Informatie wordt vanuit meerdere bronnen bij elkaar gezocht. Op dit moment kennen we geen beperkingen op het opslaan en kopiëren van bestanden op het netwerk, het mailen ervan, opslaan in een samenwerkingsomgeving (IBM Connect People).

In de architecturen is er scheiding in componenten voor massaal en toezicht. Interactie staat sowieso apart. In de BPM toepassingen is er sprake van toegang afhankelijk van de rol van de medewerker. In Java applicaties wordt vaak gedifferentieerd tussen wat groepen gebruikers mogen zien en doen, ook al is het op basis van maatwerk.

De informatiehuishouding van de Belastingdienst is omvangrijk en bevat een zeer groot aantal documenten. De autorisatie is op een hoog niveau ingeregeld. De informatieobjecten en documenten zijn geen onderdeel zijn van het klantdossier.

De Need to know implementatie raakt:

- > 400 door de IV organisatie ontwikkelde en beheerde applicaties;
- > 100 door de business ontwikkelde en beheerde applicaties;
- > 600 werkprocessen;
- > 7.000 datagebieden (zoals databases, dataopslag, datasilo's en dataformaten);
- > 2 miljard documenten.

De Belastingdienst maakt daarbij gebruik van een grote variëteit aan ontwikkelomgevingen.

5.2 Afscherming gegevens

De Belastingdienst schermt de gegevens van bepaalde groepen personen in het bijzonder af:

- Afscherming van VIP's. In de basisregistratie voor personen (BVR) staan ook gegevens van personen die zijn geclassificeerd als VIP. Deze mogen alleen door daartoe geautoriseerde gebruikers worden ingezien.
- Afscherming op medewerkers (collega's). Medewerkers in dienst van de Belastingdienst zijn ook alle geregistreerd in de basisregistratie. Het is onwenselijk dat gegevens van collega's kunnen worden ingezien.
- Afscherming van ondernemingen, beursgenoteerd of anderszins. De gegevens van beursgenoteerde ondernemingen worden afgeschermd om misbruik van deze gegevens te voorkomen, bijvoorbeeld bij handel met voorkennis.
- Fraude posten. De gegevens van personen die meewerken in een fraudeonderzoek zijn afgeschermd.
- Tonen subset van gegevens op basis van gebruikersprofiel, waarbij het hier gaat om subsets van eigenschappen van een record als ook om subsets van records van een bepaald type (bijvoorbeeld uit de set van alle klanten de subset van klanten die in provincie Gelderland wonen).
- Ten behoeve van klantbeeld is een autorisatie mechanisme ontwikkeld op basis waarvan medewerkers een subset het totaal van klantgegevens kunnen (in)zien op basis van hun profiel.
- Afscherming op de werkvoorraad van de workflow bij BPM – toepassingen. Op de werkvoorraad van de kantoorapplicaties kunnen autorisaties worden gezet op basis van identificatie en rol.
- Beheerfunctionaliteit. De functionaliteit om autorisaties en rollen te zetten of te wijzigen verschilt per toepassing.

De afscherming van gegevens is op dit moment als volgt geïmplementeerd:

- Voor de Windows omgeving is de benodigde afscherming op basis van bovenstaande regels toegepast m.b.v. active directory groepen en rol-gebaseerde toegang voor gebruikers, vastgelegd in een Identity management system (IMS). Deze active directorygroepen worden ook gebruikt voor de verschillende werkvoorraden van de kantoor applicaties.
- Op de mainframe omgeving is ook rol-gebaseerde afscherming ingesteld op basis van het RACF (Resources Acces Control Facility) systeem.
- Indien gebruik gemaakt wordt van het Identificatie-authenticatie mechanisme wordt dit gelogd. Bij een aantal systemen worden ook binnen de systemen uitgevoerde activiteiten gelogd.

Hoofdstuk 6. Gewenste situatie

6.1 Gewenste omgeving

De Belastingdienst heeft op basis van de huidige inzichten een mogelijk beeld gevormd van de gewenste omgeving. In hoofdstuk 8 zijn een aantal use cases beschreven.

Aanvullend geven we in de onderstaande paragrafen een high-level beeld van de gewenste omgeving.

De behandelaar van een zaak beperkt zich niet tot het behandelteam, de unit of medewerkers van een bedrijfsonderdeel maar kan in principe elke medewerker van de Belastingdienst met de daartoe benodigde expertise zijn.

Naast de geautoriseerde behandelaars en/of belastingplichtige voor het klant dossier kan het zaakdossier (na concrete toewijzing) worden ingezien en gemuteerd door de behandelaar(s) van de zaak. Na afronding van de zaak dient de autorisatie voor de behandelaars te vervallen en beperkt deze zich tot de geautoriseerde van het behandelteam/-unit.

In onze ideaal situatie heeft de medewerker “op maat” zonder aanvullend acties alle noodzakelijke informatieobjecten beschikbaar die de medewerker nodig heeft en waar de medewerker toegang toe heeft. Voor het geval de behandeling vereist dat er extra informatie aan de zaak wordt toegevoegd moet dit binnen restricties mogelijk zijn voor de behandelaar.

6.2 Informatiebeveiliging

De Belastingdienst moet traceerbaar en zorgvuldig omgaan met de privacy en informatie van burgers en ondernemers. De basis hiervoor is een compliance werkomgeving voor de medewerker. De eisen vanuit wetgeving aan de informatiebeveiliging worden zwaarder. Tevens is de publieke opinie omtrent de informatiebeveiliging en toegang tot informatie aan het veranderen en er is meer aandacht/toezicht op informatiebeveiliging vanuit de politiek op de Belastingdienst.

In de eindsituatie hebben alle medewerkers een werkomgeving ter beschikking waar het werk optimaal uitgevoerd kan worden zonder dat de medewerker zich zorgen hoeft te maken over het al dan niet voldoen aan wet- en regelgeving. De medewerker heeft alleen toegang en autorisatie tot systemen en informatie conform de rol van de medewerker en wat nodig is voor het uitvoeren van de taken op dat moment en niet meer dan dat. Dit willen we gaan realiseren door gebruik te maken van een volgende stap bij het inzetten van de beveiligingsconcepten *Need to know* en *Zero trust*.

6.3 Need to know en Zero trust.

Need to Know en Zero trust is feitelijk het invullen van de “eisen van aantoonbaarheid”. Een gebruiker krijgt toegang tot een beperkte set aan informatie, mits we zeker weten dat hij is wie hij beweert te zijn. Conform Zero trust mag een gebruiker bij default helemaal niets.

De door ons nu onderkende basis beveiligingsconcepten van Need to Know en Zero trust zijn:

1. Identificatie, authenticatie
Ben je wie je zegt dat je bent en op zo ja dan krijg de medewerker toegang.
De locatie waar de medewerker zich bevindt is mede bepalend voor de verkregen toegang.

2. Autorisatie

- a. Rol gebaseerde toegang waarbij medewerkers op basis van hun ID, rol en (semi) real time afhankelijk van tijd, plaats en apparaat toegang tot Belastingdienst omgeving en de Belastingdienst systemen.
- b. Attribuuat gebaseerde toegang waarbij een medewerker op basis van zijn ID, rol, en toegewezen zaken toegang heeft tot gegevens geleverd door een service of applicatie (claim based autorisatiemodel).
- c. Rule based access control. Een medewerker heeft op basis van business rules toegang tot zaken, taken en gegevens binnen de zaken en taken.
- d. Actief vragen naar toegang (purpose-based credentials). Toegang vragen, geautomatiseerd vastleggen en loggen op het moment dat het nodig is.
- e. Gebruik van DigiD voor burgers en eHerkenning voor ondernemers.

De locatie waar de medewerker zich bevindt is mede bepalend voor de verkregen autorisatie.

3. Pseudonimiseren - Anonimiseren

Hiernaast onderkennen we pseudonimiseren- Anonimiseren (data hiding). Dit willen we gaan aanbieden in situaties waar het voor de medewerker belangrijk is om te weten welke informatie beschikbaar is zonder direct toegang tot deze informatie te hebben. Een optie hierbij is dat de medewerker alleen ziet dat informatie beschikbaar maar deze niet kan inzien.

4. Actieve monitoring

Aanvullend wil de Belastingdienst de risico-beperkende maatregelen actieve real-time monitoring, actieve signalering en blokkeren op basis van real-time sensor-data onderzoeken. Dit richten we dan proportioneel in met een differentiatie op rol en toegewezen dossiers.

Randvoorwaarde bij het gebruik van beveiligingsconcepten is dat herleidbaarheid van handelen altijd gewaarborgd blijft, ook bij de inzet van robots. Alle handelingen zijn onweerlegbaar herleidbaar tot (de verantwoordelijkheid van) een natuurlijk persoon conform de BIO en iBB 3.2.2 punt b.

De door de deelnemende marktpartij voorgestelde oplossing moet kunnen samenwerken met een grote variëteit aan bij de Belastingdienst in gebruik zijnde ontwikkelomgevingen zoals Cobol, Java Power/builder Sydebase en DotNet. en de technologische platformen zoals z/OS, Linux, Windows, BPM, Filenet, DB2, Teradata, SAP.

6.4 Uitgangspunt voor de werkplek van de medewerker.

De Belastingdienst biedt de medewerkers een werkomgeving waarin zij hun werk optimaal kunnen uitvoeren zonder zich zorgen te hoeven maken over het al dan niet voldoen aan wet- en regelgeving.

6.5 De compliance werkomgeving

De Need to know en Zero trust beveiligingsconcepten willen we gaan toepassen in de werkomgeving van de medewerker. De hoofdcomponenten waar de werkomgeving van de medewerker uit gaat bestaan zijn:

Zaakgericht werken:

- Een centrale plek/toegang tot zaken waar hij voor geautoriseerd is, onafhankelijk van het proces;
- Informatie op maat (wat moet hij weten om zijn werk te kunnen doen);
- Verschillende afdelingen/teams kunnen samenwerken aan de zaakbehandeling, ze delen de beschikbare informatie.

Zaakadministratie:

- Als de medewerker zijn persoonlijke omgeving gebruikt voor het werken aan een dossier, is dit altijd onder de besturing van document management die gedurende de gehele levensduur van een document (creatie, bewerken, definitief, archiveren, verwijderen) de status van dit document kent en managet de informatie wordt dan altijd centraal opgeslagen en niet op de persoonlijke omgeving.

Zaakdossier:

- Gegevens worden gemeenschappelijke opgeslagen binnen applicaties en in het document management systeem. Er is geen andere omgeving waar deze gegevens opgeslagen kunnen worden;
- Er is een gedeelde informatiepositie met burgers en ondernemers;
- Bijzondere gegevens conform (AVG) zoals strafrecht of medische gegevens moeten op basis van een hogere classificatie extra afgeschermd opgeslagen kunnen worden.

6.6 Informatie uitwisseling met belastingplichtigen

De Belastingdienst wil, conform de wetgeving, op toegankelijke wijze, belastingplichtigen toegang geven tot:

Klantdossier:

- Elke belastingplichtige (burger/ondernemer (subject)) heeft een klantdossier als een bundeling van informatieobjecten.

Klantcontactdossier:

- Elke belastingplichtige heeft een contactdossier met alle in- en uitgaande contacten over alle kanalen en inzicht in de track & trace informatie op uitgewisselde berichten.

Gedeelde informatiepositie:

- Het delen van informatie tussen belastingplichtige en de Belastingdienst om de afhankelijk van de overheid te verminderen. De informatiepositie van de burgers/ondernemers komt hiermee op een gelijkwaardiger niveau ten opzichte van de Belastingdienst.

6.7 Inrichting vertrouwelijkheidsservice bij de werkomgeving van de medewerker

De Belastingdienst werkt met klantendossiers die bestaan uit een klant begeleidingssysteem en de onderscheiden zaakdossiers.

De afscherming van de gegevens in de klantendossiers is gebaseerd op de 2 soorten klanten, de gevoelige- en reguliere entiteiten, die de Belastingdienst onderkent.

- Voor de gevoelige (beursgenoteerde, top 100 en grote ondernemingen) entiteiten moet de afscherming op klantdossier beperkt worden tot het specifiek benoemde behandelteam;
- Voor reguliere klanten moet de afscherming tot medewerkers van een unit kunnen plaatsvinden. Een klantdossier kent een beperkt aantal vaste behandelteams.

In de gewenste situatie werkt de Belastingdienst met een inrichting waarbij informatieobjecten alleen kunnen worden ingezien indien de behandelaar hiervoor de juiste autorisatie heeft. De gewenste oplossing moet kunnen omgaan met informatieobjecten die; in een of meerdere systemen zijn opgeslagen, eenmalig worden opgeslagen, en in meerdere dossiers relevant en beschikbaar zijn.

Hoofdstuk 7. Vragen

Vragen	
Vraag 1.	Visie - Wat is uw visie ten aanzien van de beveiligingsconcepten Need to know en Zero trust (zoals opgenomen in paragraaf 4.6.2)? - Worden er door u nog andere beveiligingsconcepten onderkend welke relevant zijn voor de door ons benoemde hoofdgebieden?
Vraag 2.	Beveiligingsconcepten Welke beveiligingsconcepten, ondersteunt de door u voorgestelde oplossing en op welke manier?
Vraag 3.	Doelmatig Geef aan wat de doelmatigheid is van de door u ondersteunde beveiligingsconcepten?
Vraag 4.	Best practices en patronen Welke best practices en patronen heeft u beschikbaar.
Vraag 5.	Ervaringen Welke ervaringen heeft u met de implementatie van Need to know en zero trust bij vergelijkbare organisaties.?
Vraag 6.	Welke mogelijkheden ziet u voor de autorisatie op lager niveau (medewerker, transactie, data) in legacy systemen?
Vraag 7.	Omgeving - Is uw oplossing on-premise en/of als SaaS dienst beschikbaar? - Welke voor en nadelen hebben deze twee omgevingen ten opzichte van elkaar?
Vraag 8.	Organisatie inrichting Geef aan hoe de Belastingdienst organisatie ingericht dient te worden om de Need to know en Zero trust met uw product bij de Belastingdienst optimaal in te kunnen zetten.
Vraag 9.	Beheer inspanningen Welke beheersinspanning is nodig en hoe kan de organisatie ingericht worden om die inspanning zo laag mogelijk te houden?
Vraag 10.	Op welke manier wordt geborgd dat de voorgestelde oplossing efficiënt voor de medewerker en belastingplichtige wordt ingezet?
Vraag 11.	Bestaande systemen Hoe kan de voorgestelde oplossing toegepast worden bij bestaande (en deels verouderde) systemen/technologieën (zie paragraaf 6.3) en waar dient de Belastingdienst rekening mee te houden?
Vraag 12.	Implementatie Met welke doorlooptijden, inzet, en risico's hebben wij ten aanzien van een implementatie bij de Belastingdienst rekening te houden?
Vraag 13.	Afhankelijk van tijd, plaats en apparaat toegang tot Belastingdienst omgeving Toegangsrechten tot dossiers en zaken zijn naast de rol van de medewerker ook afhankelijk van de locatie waar de medewerker toegang tot deze informatie vraagt. Geef aan hoe u product een oplossing biedt voor locatie afhankelijke toegang.

Vragen	
Vraag 14.	Use cases (hoofdstuk 8) Geef aan op welke wijze uw voorgestelde oplossing invulling kan geven aan de beschreven use cases (zoals opgenomen in hoofdstuk 8). Geef hierbij duidelijk aan welke van de door ons onderkende vier, basis beveiligingsconcepten Need to know en Zero trust (zoals opgenomen in paragraaf 6.3) hierbij toegepast worden?
Vraag 15.	Integratiemogelijkheden Over welke mogelijkheden en integratie oplossingen met DigID en E-Herkenning beschikt uw oplossing voor externe gebruikers zoals ondernemingen en burgers (Belastingdienst en onderneming/burger beschikt over dezelfde informatie). Hoe werkt dit?
Vraag 16.	Ontbrekende vragen Zijn er belangrijke onderwerpen welke we niet gevraagd hebben, maar waar we volgens u wel rekening mee moeten houden?
Vraag 17.	Kostenindicatie Met welke kosten en kostenelementen dienen wij rekening te houden? Te denken valt aan onder andere: • Implementatiefase ○ Inrichting/configuratie ○ Realisatie koppelingen en interfaces • Operationele fase ○ Gebruik van de voorgestelde oplossing Op basis van welke variabelen (zoals (named) users, aantal transacties en enterprise) kan het gebruik worden afgenomen ○ Beheer, onderhoud en support
Vraag 18.	Product demonstratie: a. Bent u bereid om een demonstratie te verzorgen? b. Zijn er aanvullende voorwaarden verbonden aan de demonstratie? Zo ja welke?
Vraag 19.	Proof of Concept: a. Bent u bereid om mee te werken aan een uitgebreide Proof of Concept? b. Zijn er aanvullende voorwaarden verbonden aan de Proof of Concept? Zo ja welke? c. Wenst u gebruik te maken van de vergoeding voor het uitvoeren van de Proof of Concept? Zo ja, graag ontvangen wij een indicatie van de vergoeding (zoals beschreven in paragraaf 3.8).

Tabel 4. Vragen

Hoofdstuk 8. Use cases

Onderstaande use cases geven een actueel en realistisch beeld van de huidige problematieken bij de Belastingdienst. Deze use cases dienen tevens gebruikt te worden voor de beantwoording van deze marktconsultatie.

Medewerker Belastingdienst	
Use case 1.	Een medewerker logt thuis in, in een Aangifte systeem. a. De medewerker kan de volledige Aangifte van een organisatie wel inzien, b. De medewerker mag het bijbehorende dossier niet aanpassen.
Use case 2.	De medewerker reist met de trein van huis naar kantoor. In de trein werk hij op een mobiele werkplek. a. De medewerker kan in de trein een notitie opstellen, b. De medewerker kan in de trein een Aangifte en het bijbehorende dossier Niet inzien.
Use case 3.	Op kantoor logt de medewerker weer in, in een Aangifte systeem. a. De medewerker kan de volledige Aangifte en het dossier van een organisatie wel inzien, b. De medewerker mag het volledige dossier van de Aangifte inzien en aanpassen.
Use case 4.	De medewerker heeft voor het behandelen van Aangiften een andere rol met meer rechten gekregen. De medewerker logt op kantoor in op de applicatie "Inzicht" a. Binnen de applicatie Inzicht kan de medewerker nu de aangifte van Zeer vermogende Personen wel behandelen.
Use case 5.	Ik ben klantmanager bij Douane a. Als ik in de provincie Groningen ben mag ik van alle klanten van de regio Groningen de dossiers inzien, b. Als ik buiten de provincie ben mag ik rubrieken gekenmerkt als fraude gevoelig niet (meer) inzien.
Use case 6.	Op Schiphol wordt iemand gearresteerd die in bezit is van grote hoeveelheden sigaretten en 100 gram cocaïne. Het opgemaakte proces-verbaal bevat informatie over dit strafbaar feit. a. Als Belastingdienst ambtenaar mag ik van het proces-verbaal alleen de informatie over de sigaretten zien, b. Als Bijzondere opsporingsambtenaar mag ik het gehele proces-verbaal inzien.

Tabel 5. Use cases medewerker Belastingdienst

Aangifte behandelaar Particulieren (P)	
Use case 7.	Als behandelaar IB (inkomstenbelasting) behandel ik de IH (inkomstenheffing) aangifte 2019 van dhr. A. en mevr. B. Dhr. A en mevr. B zijn fiscaal partners maar doen afzonderlijk aangifte. Voor de behandeling zijn deze aangiften separate "zaken". a. Voor de Aangifte behandeling wil ik de Aangifte van dhr. A. beoordelen en opmaken, b. Omdat de partners afzonderlijk aangifte doen wil ik ook de aangifte van mevr. B behandelen.

Aangifte behandelaar Particulieren (P)	
Use case 8.	Als behandelaar IB behandel ik een andere IH aangifte 2019 Ik zie dat er hoge ziektekosten zijn opgevoerd in de Aangifte. - Ik heb geen toegang tot medische informatie in het dossier. Ik heb wel toegang tot de financiële informatie rondom de ziektekosten, - De burger heeft met behulp van DigiD toegang tot het dossier en heeft de mogelijkheid om aanvullende informatie in het dossier op te voeren.
Use case 9.	Voor het beoordelen van de juistheid van de Aangifte is toegang tot de medische informatie noodzakelijk. - De medewerker vraagt een collega om assistentie, - De medewerker vraagt zelf om tijdelijk, gedurende de looptijd van het dossier, extra toegangsrechten.
Use case 10.	Als behandelaar IB behandel ik een IH aangifte 2019 van dhr. C. Ik krijg een signaal dat het vermogen van de dhr. C een extra beoordeling moet krijgen. Hiervoor start ik de applicatie Klantbeeld. Het Klantbeeld systeem toont precies de informatie die ik mag zien en die ik nodig heb.

Tabel 6. Use cases Aangifte behandelaar Particulieren (P)

Toezicht medewerker Grote Ondernemingen (GO)	
Use case 11.	Als toezichtmedewerker beoordeel ik aangifte van alle Grote ondernemingen. Ik heb privé aandelen Shell gekocht. Vanuit handelen met voorkennis mag ik zolang ik deze aandelen in bezit heb geen koersgevoelige informatie, deel van het dossier, over Shell meer (in)zien.
Use case 12.	Als toezichtmedewerker beoordeel ik een aangifte. Het hierbij opgebouwde dossier is inzichtelijk voor de klant uitgezonderd het onderdeel potentiële fraude. - Als klantcoördinator wil ik een opdracht en rechten geven om een aangifte te behandelen - De aangever heeft met eHerkenning toegang tot het gedeelde deel van het dossier.

Tabel 7. Use cases Toezicht medewerker Grote Ondernemingen (GO)

Aangifte behandelaar Midden en Kleinbedrijf (MKB)	
Use case 13.	Als behandelaar VPB behandel ik de VPB aangifte 2020 van bedrijf XYZ - Hiervoor wil ik de aangifte VPB 2020 beoordelen en opmaken, - Ter controle wil ik ook de VPB aangifte 2019 inzien.
Use case 14.	Als toezichtbehandelaar controleren we een aantal cafés op omzet. We hebben toestemming nodig en gevraagd voor onderzoek bij cafés A, B, C en D Ter plekke constateren we dat café X ook onderzocht zou moeten worden. We hebben hiervoor geen rechten. Welke opties zijn mogelijk voor het uitbreiden van het onderzoek en het verkrijgen van bijbehorende rechten.

Tabel 8. Use cases Aangifte behandelaar Midden en Kleinbedrijf (MKB)

Bijzondere situaties	
Use case 15.	Een medewerker vraagt ineens herhaaldelijk extra toegang tot onderdelen van dossiers a. Voordat handmatig naar deze aanvragen is gekeken is de extra toegang tot dossiers voor deze medewerker ingetrokken en krijgt de Teamleider een signaal.
Use case 16.	Een medewerker opent op de Belastingdienst werkplek thuis in de nacht van zaterdag op zondag een aangifte van een Grote onderneming. a. De combinatie van het tijdstip van deze actie en organisatie wordt automatisch gesignaleerd, als risico gemarkeerd en automatisch afgebroken.
Use case 17.	Een robot voert geautomatiseerd wijzigingen door in een middleware systeem a. De herleidbaarheid van handelen dient hierbij geborgd te blijven.
Use case 18.	Een medewerker wil op een 'onderdeel' van een dossier een bewerking, kopiëren, aanpassen, mailen, opslaan in een samenwerkingsomgeving of op zijn persoonlijke werkplek, uitvoeren. a. Afhankelijk van de ingestelde beperkingen op het 'onderdeel' en rechten kan de medewerker deze bewerking daadwerkelijk uitvoeren.
Use case 19.	Beveiliging digitaal archief. De robot Watson zoekt in het digitaal archief naar informatie. a. Het resultaat van de zoekopdracht mag niet meer zijn dan waar de opdrachtgever toe geautoriseerd is.

Tabel 9. Use cases bijzondere situaties