



Belastingdienst

Aansluitvoorwaarden LTB

Versie 1.1

Colofon

Dit document is een uitgave van:

Belastingdienst
SSO Financieel & Managementinformatie

Logisch ToegangsBeheer (LTB) en Functioneel Beheer Bedrijfsvoering
(FB/BV)

John F. Kennedylaan 8 | 7314 PS Apeldoorn | gebouw E, 4e etage
Postbus 599 | 7300 AN Apeldoorn

Inhoudsopgave

1	Documentbeheer 3
1.1	Documenthistorie 3
1.2	Beheer document 3
1.3	Reviewers 3
2	Algemeen 4
2.1	Leeswijzer 4
3	Inleiding 5
3.1	Kaders en richtlijnen 5
4	Toelichting LTB proces 6
4.1	<i>Identificatieproces: Gebruikers aansluiten op IMS 6</i>
4.2	Autorisatieproces: IMS rollenmodel 6
4.2.1	Permissies en groepen 6
4.2.2	Rollenmodel 7
4.2.3	Functiescheiding (SOD) 7
4.3	Authenticatieproces: Aansluiten wachtwoord 8
5	Aansluitvoorwaarden 9
5.1	Aansluiten op IMS 9
	Naamgeving permissies 9
5.1.1	Autorisatiebron aansluiten op IMS, automatische koppeling 10
5.1.2	Autorisatiebron aansluiten op IMS, handmatige koppeling 10
5.1.3	Autorisatie Informatie 11
5.2	Applicatie beschikbaar maken in het LTB proces (formulieren) 11
5.3	Checklist voor het aansluiten op IMS 12
6	Bijlage 1: Aanvraagformulieren 13
7	Bijlage 2: Indeling csv-bestand voor IST informatie. 14
8	Bijlage 3 : Afkortingen 15
9	Bijlage 4 : Begrippen en definitie 16

1 Documentbeheer

1.1 Documenthistorie

Versie	Datum	Status
0.1	Juli 2020	1 ^e concept nieuwe versie
0.2	November 2020	Concept, 1 ^e review verwerkt
0.3	Februari 2021	Reviews team FB/BV2 verwerkt
0.4	Mei 2021	Reviews team Rollenbeheer en APK verwerkt
0.7	September 2021	Aanpassing formulier A via RFF
1.0	November 2021	1.0 versie voor publicatie op intranet
1.1	November 2022	Naamgevingsconventie permissie toegevoegd

1.2 Beheer document

Het beheer van dit document is belegd binnen SSO F&MI, team LTB en FB/BV. Zij zijn verantwoordelijk voor het opstellen en wijzigen van dit document.

1.3 Reviewers

Naam	Rol	Organisatie onderdeel
Christian Londero	Advies, Proces en Kwaliteit	SSO F&MI
Erik Sluis	Functioneel Beheer Bedrijfsvoering 2	SSO F&MI
Team FB/BV2	Functioneel Beheer Bedrijfsvoering 2	SSO F&MI
Team Rollenbeheer	Rollenbeheer	SSO F&MI
Team APK	Advies, Proces en Kwaliteit	SSO F&MI

2 Algemeen

Dit document gaat over de aansluitvoorwaarden Logisch ToegangsBeheer (LTB), ook wel Identity & Acces Management (IAM) genoemd. De aansluitvoorwaarden vormen de requirements, waaraan applicaties en informatiesystemen moeten voldoen om opgenomen te kunnen worden in het LTB proces.

2.1 Leeswijzer

Het document begint met een inleiding (hoofdstuk 3) en een toelichting op het LTB proces (hoofdstuk 4). Indien er weinig tot geen kennis van het LTB proces aanwezig is wordt aangeraden deze hoofdstukken ook door te nemen. In hoofdstuk 5 worden de daadwerkelijke aansluitvoorwaarden voor het aansluiten van een applicatie op IMS beschreven. Hoofdstuk 5.3 bevat een checklist aan de hand waarvan gecontroleerd kan worden of de benodigde stappen doorlopen zijn.

3 Inleiding

Het proces van het beheer van medewerker autorisaties (verstrekken, intrekken en controleren) wordt binnen de Belastingdienst Logisch Toegangsbeheer genoemd, afgekort LTB. Een meer algemeen bekende term hiervoor is Identity & Acces Management (IAM). Het LTB-proces omvat het identificatieproces, autorisatieproces en het authenticatieproces. Voor een gecontroleerd LTB-proces is het noodzakelijk dat alle ICT-voorzieningen die autorisaties bevatten, de autorisatiebronnen, aangesloten zijn of worden op het LTB-proces. Immers, wanneer autorisaties niet bekend zijn binnen het LTB-proces, kunnen deze ook niet vanuit het LTB-proces worden ondersteund. Een ander autorisatieproces dan het LTB-proces is er niet binnen de Belastingdienst. Hoewel de ambitie is om ook de Ontwikkel-, Test-, en Acceptatieomgevingen aan te sluiten op IMS, gaan de aansluitvoorwaarden op dit moment alleen over de productieomgeving.

3.1 Kaders en richtlijnen

De kaders en richtlijnen zoals beschreven in dit document gelden voor alle applicaties en informatiesystemen die in het Belastingdienst domein door Belastingdienst medewerkers gebruikt worden.

Doelgroep

De LTB aansluitvoorwaarden gelden voor:

1. Informatiemanagers
2. Projectmanagers
3. Ontwerpers van processen, systemen en applicaties
4. Ontwikkelaars van systemen en applicaties
5. Beheerders van systemen en applicaties
6. Architecten
7. Business Analisten
8. Leveranciers en andere overheden welke applicaties ontwikkelen voor gebruik door belastingdienst medewerkers.

4 Toelichting LTB proces

Het LTB proces wordt ondersteund door de applicatie IMS; Identity Management System. IMS bevat (o.a) usernames (identiteiten) en autorisaties. Autorisaties worden in IMS beschikbaar gesteld in rollen volgens de Role Based Acces Control (RBAC) methodiek. Zodra een nieuwe applicatie beschikbaar komt, moeten leidinggevendende medewerkers kunnen autoriseren door het toekennen van rollen in IMS. Door het toekennen van rollen in IMS geeft de manager goedkeuring voor het gebruiken van de autorisatie door de medewerker.

Als een autorisatie niet ingericht is in IMS, dus niet opgenomen is in een rol, dan kan deze ook niet ter beschikking worden gesteld aan de medewerker. Onderstaand een uitgebreidere toelichting op het identificatie-, autorisatie- en authenticatieproces.

4.1 Identificatieproces: Gebruikers aansluiten op IMS

Het P-proces levert aan het LTB-proces alle relevante gegevens van de medewerkers die voor de Belastingdienst werken. Van deze gegevens worden usernames (identiteiten) gegenereerd en geadministreerd in IMS. Een username wordt gebruikt om een useraccount te creëren in een applicatie of op een doelsysteem. De username is hiermee herleidbaar naar een natuurlijk persoon.

Naast de reguliere aanlevering van medewerker gegevens vanuit het P-proces zijn er in de praktijk ook uitzonderingsgevallen. Dit betreft o.a.

- Medewerkers van zogenaamde Vertrouwde Derden, partijen waar de Belastingdienst mee samenwerkt of die informatie van de Belastingdienst behoeven.
- Medewerkers van Ketenpartners die binnen een bedrijfsonderdeel van de Belastingdienst werkzaam zijn.
- Tijdelijke persoonlijke username, voor bv campagne werkzaamheden (deze worden steeds minder gebruikt, vanwege het automatisch genereren van usernames vanuit het P-proces).
- Systeem accounts die nodig zijn om de systeemprocessen draaiende te houden. *(deze worden Functionele accounts genoemd)*.
- Personas (extra userID gekoppeld aan het eigen userID van de medewerker).

Deze categorieën worden handmatig beheerd en geregistreerd in IMS.

4.2 Autorisatieproces: IMS rollenmodel

Nieuwe of gewijzigde applicaties dienen tijdig aangemeld te worden bij SSO F&MI, Functioneel Beheer Bedrijfsvoering team 2. Functioneel Beheer Bedrijfsvoering team 2 zorgt ervoor dat de applicatierollen als permissies worden opgenomen in IMS. Hiervoor dient de applicatie te voldoen aan de aansluitvoorwaarden, zie hoofdstuk 5. Zodra de permissies zijn vastgelegd in IMS kunnen deze opgenomen worden in het rollenmodel voor de diverse organisatieonderdelen.

4.2.1 Permissies en groepen

Permissies geven inhoud aan de rollen. Permissies bevatten de daadwerkelijke behoeften (groepen) om iemand te autoriseren voor een rol in de applicatie. Permissies kunnen, afhankelijk van de situatie, opgenomen worden in bestaande rollen of er kunnen nieuwe rollen gemaakt worden.

Een permissie bevat in principe 1 groep. Een groep is de technische representatie in doelsystemen van applicatierollen of toegangsrechten, ook wel group of technische benodigdheden genoemd. Vanuit de voortbrenging moet bij LTB, Functioneel Beheer Bedrijfsvoering team 2 (FB/BV2) aangegeven worden welke groepen er zijn binnen de applicatie en welke permissies (applicatierollen) er voor deze groepen aangemaakt moeten worden, oftewel het opleveren van de autorisatiematrix.

4.2.2 **Rollenmodel**

Tijdens het ontwerpen van een proces dient te worden aangegeven welke functies en rollen binnen dit proces worden onderkend. Hierbij moet er rekening worden gehouden met functiescheidingen, risico's en ongeautoriseerde toegang. Elk bedrijfsonderdeel legt vast welke autorisaties een user nodig heeft in zijn rol, volgens het "need to do"¹ en "need to know"² principe. Het voor het proces verantwoordelijke management geeft aan welke rollen nodig zijn, met de daarbij behorende autorisaties. De proceseigenaar geeft ook aan wat de beoogde doelgroep is en welke autorisatie voor welke functionaris bedoeld is. Dit gebeurt in samenspraak met de adviseur informatiebeveiliging van het betreffende bedrijfsonderdeel. Deze informatie wordt verstrekt aan team FB/BV2.

Team rollenbeheer stelt, in afstemming met de adviseur informatiebeveiliging, vast wat de risicoclassificatie is van de rol, op basis van de geleverde informatie vanuit het project of procesverantwoordelijke. Risico's worden ingedeeld naar 'geen risico', 'risico met alleen berichtgeving' of 'risico met goedkeuring nodig'. Daarnaast stellen ze vast of de rol automatisch toegewezen mag worden. Daarvoor bepalen ze de afleidingsregel waaraan de gebruiker moet voldoen om de rol te krijgen. Team rollenbeheer voert op, verwijdt of muteert de rol in IMS.

4.2.3 **Functiescheiding (SOD³)**

Bij het ontwerpen van een nieuwe applicatie dient rekening gehouden te worden met functiescheiding binnen de applicatie. Zo mag een gebruiker niet de mogelijkheid hebben om bijvoorbeeld tegelijkertijd te kunnen heffen en innen of muteren en autorisaties toekennen.

Daarnaast stelt de proceseigenaar, in overleg met de adviseur informatiebeveiliging, vast welke combinaties van autorisaties tussen de verschillende applicaties risicovol zijn en levert dit als SOD-regel aan bij afdeling LTB, Functioneel Beheer Bedrijfsvoering team 2 (FB/BV2). Dit wordt vervolgens vastgelegd in IMS. Deze SOD-regels bestaan altijd uit een combinatie van twee permissies die conflicterend zijn.

Bij het opstellen van rollen met bijbehorende autorisaties dient een scheiding gemaakt te worden tussen de functies beschikken, bewaren, registreren, uitvoeren en controleren. De combinatie van autorisaties, die de functiescheiding doorbreken, mogen nooit in één rol voorkomen.

¹ *Need to do: autoriseren van medewerkers tot het raadplegen en verwerken van die gegevens, het binnentreden van die ruimten en het gebruik van die middelen, die zij voor hun werk nodig kunnen hebben.*

² *Need to know: het vertrouwen in de eigen medewerkers, die bedrijfsmiddelen gebruiken waarvoor ze bedoeld zijn. Ze raadplegen alleen die gegevens en gebruiken alleen die ruimten of middelen die ze nodig hebben.*

³ SOD = Segregation Of Duties, oftewel scheiding van taken (functiescheiding).

4.3 Authenticatieproces: Aansluiten wachtwoord

Voor alle systemen/programma's waarvoor een wachtwoord nodig is dient er initieel een sterk wachtwoord aangemaakt te worden door de autorisatiebeheerder van de applicatie. Het resetten van de wachtwoorden kan door verschillende partijen, servicedesk of centrale autorisatiebeheerders, of geautomatiseerd gebeuren. Ook zij dienen een sterk wachtwoord uit te geven. Lees meer over wachtwoordconventies in het Handboek Beveiliging Belastingdienst (HBB) hoofdstuk C.13.7.3 wachtwoordconventies:

Implementatierichtlijnen

a) Wachtwoorden voldoen aan de volgende wachtwoordconventie:

1. minimaal acht tekens;
2. minimaal één hoofdletter;
3. minimaal 4 kleine letters;
4. minimaal 1 cijfer en/of één vreemd teken;
5. nieuw wachtwoord moet in minimaal twee tekens verschillen met het vorig wachtwoord.

b) Wachtwoorden van gebruikersaccounts moeten minimaal elke 90 dagen gewijzigd worden.

c) Wachtwoorden van functionele accounts worden minder frequent gewijzigd, namelijk minimaal eens per jaar en ten minste bij elke nieuwe release van de IT service, maar daarentegen zijn de wachtwoorden langer, namelijk minimaal 20 posities, met willekeurig gekozen cijfers, tekens en speciale tekens.

d) De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij geldt het volgende:

1. Voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthenticeerd;
2. ter voorkoming van typefouten in het nieuw gekozen wachtwoord is er een bevestigingsprocedure;
3. alvorens een nieuw wachtwoord wordt gewijzigd, wordt geautomatiseerd gecontroleerd of het nieuwe wachtwoord aan de vereiste conventies voldoet.

e) De default en installatiewachtwoorden worden tijdens of direct na installatie verwijderd of gewijzigd.

f) Initiële wachtwoorden en wachtwoorden die gereset zijn, voldoen aan bovenstaande wachtwoordconventie en daarbij wordt door het systeem afgedwongen dat bij het eerste gebruik dit wachtwoord wordt gewijzigd.

5 Aansluitvoorwaarden

5.1 Aansluiten op IMS

Functioneel Beheer BV2 dient minimaal 6 weken voor de in productie name van de nieuwe/gewijzigde applicatie op de hoogte te worden gebracht van de nieuwe/gewijzigde applicatie en zijn autorisatiestructuur. Dit dient reeds in de ontwerp-/bouwphase plaats te vinden. Het inrichten van de applicatie in IMS en het uiteindelijk bestelbaar maken van de autorisatie voor managers kan, afhankelijk van de situatie, namelijk 1 tot 6 weken duren.

Om de applicatie op te kunnen nemen in IMS dient er een aantal gegevens aangeleverd te worden. Zo moet FB/BV2 weten welke technische groepen de applicatie kent, wat de doelgroep is en hoe we deze moeten vertalen naar permissies (applicatierollen). Deze vertaling wordt ook wel de autorisatiematrix genoemd. FB/BV2 is altijd bereid advies te geven betreffende de inrichting. Zoek hiervoor afstemming met het team via de EUM-LTB_Postbus.

Naamgeving permissies

LET OP: De permissie dient te voldoen aan de richtlijnen en naamgevingsconventie voor permissies;

Applicatie permissie (standaard)

- De naam van de permissie moet een functionele naam voor de autorisatie zijn. Gebruik van een werkwoord en zelfstandig naamwoord is hierbij leidend. Voorbeelden (fictief): Raadplegen VPB posten, Behandelen dossiers, Muteren aanslagen.
- Voor sommige autorisaties is het niet mogelijk om een werkwoord te gebruiken. Dan moet gekeken worden of een functionaris beter geschikt is. Voorbeelden: Superuser, Administrator.

Gegevenstoegang permissie

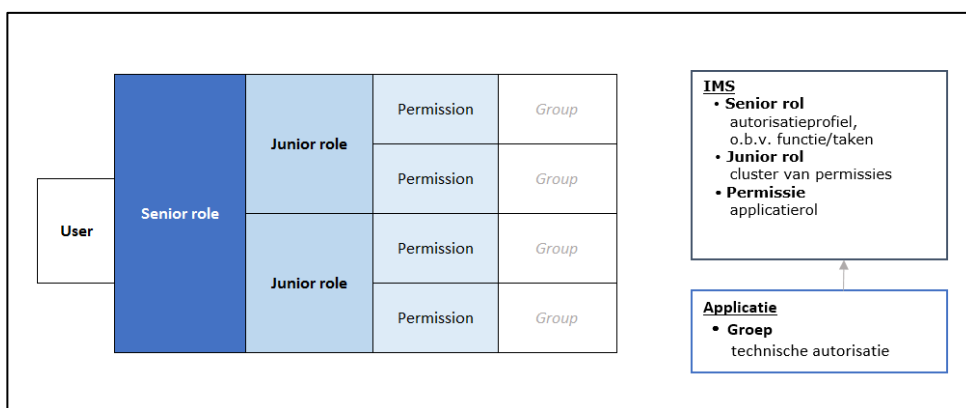
De permissies onder gegevenstoegang worden aangemaakt conform de richtlijnen van de applicatie permissies. Daarbij twee uitzonderingen:

- Samenwerkingsgebieden worden als permissie opgenomen met dezelfde naam als de groep, minus sg_
- Data toegang DNAP gebieden worden als permissie opgenomen met dezelfde naam als de groep, minus aug_

Uitzonderingen (bijv. Beheerrechten/persona)

De naam van de permissie willen we zoveel mogelijk laten voldoen aan de richtlijn van de applicatie permissie. Afhankelijk van de situatie kan in overleg met de applicatie eigenaar hiervan afgeweken worden. Dit betreft echter wel een uitzonderingssituatie. Als het voor een autorisatie niet mogelijk is om aan te sluiten op de standaard richtlijn, wat veel voorkomt bij beheer permissies, willen we een zo duidelijk mogelijk omschrijving van de werking van de autorisatie weergeven. Bij voorkeur in het Nederlands en zonder (onnodig) - en _ erin.

Een permissie kan 1 groep bevatten. Deze permissies worden vervolgens opgenomen in rollen die 1 of meerdere permissies kunnen bevatten. Voordat er permissies ingericht kunnen worden, moet er eerst autorisatie informatie (IST) worden aangeleverd zodat de groepen bekend zijn in IMS en deze opgenomen kunnen worden in permissies. Het aanleveren van deze gegevens gebeurt via een automatische koppeling of handmatig. Dit is afhankelijk van de autorisatiebron van de applicatie.



Schematische weergave van het rollenmodel; rollen, permissies en groepen

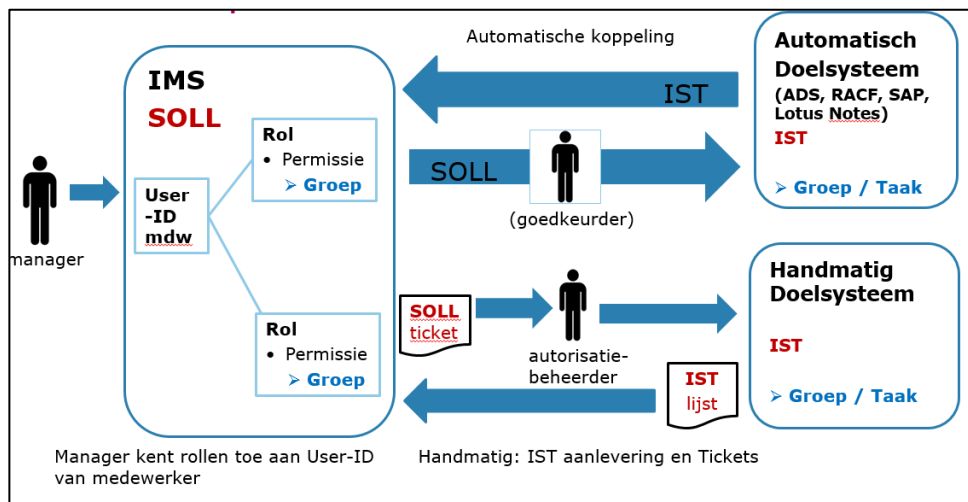
5.1.1 **Autorisatiebron aansluiten op IMS, automatische koppeling**

De applicatie dient in beginsel aan te sluiten op de autorisatiebronnen van ADS (windows), RACF (mainframe), SAP of IBM Notes (groupware en email platform). IMS heeft een automatische koppeling met deze autorisatiebronnen. Door aan te sluiten op deze autorisatiebronnen sluit je met je applicatie automatisch aan op IMS. Deze koppelingen voorzien IMS minimaal dagelijks van nieuwe autorisatie informatie (IST). Het blijft wel noodzakelijk om informatie aan te leveren voor het aanmaken van permissies (zie 5.1 en 5.2).

5.1.2 **Autorisatiebron aansluiten op IMS, handmatige koppeling**

Indien het niet mogelijk is om aan te sluiten op de genoemde autorisatiebronnen en de applicatie dus een eigen autorisatiebron heeft, dient er middels het handmatige proces aangesloten te worden op IMS. In het handmatige proces dient wekelijks autorisatie informatie (IST) uit de autorisatiebron van de applicaties aangeleverd te worden aan IMS door middel van bestandsoverdracht. Het aanmaken en aanbieden van zo'n IST-bestand dient geborgd te zijn in de applicatie(service).

De specificaties waaraan het bestand moet voldoen, staan beschreven in Bijlage 2: Indeling csv-bestand voor IST informatie.



Schematische weergave automatische koppeling/ handmatige koppeling

5.1.3 Autorisatie Informatie

Bij het automatisch dan wel handmatig aansluiten van een applicatie op IMS, wordt IMS voorzien van autorisatie informatie betreffende deze applicatie. Onder autorisatie informatie wordt verstaan: alle groepen en accounts met lidmaatschappen zoals deze voorkomen in de autorisatiebron van de applicatie.

Groepen: unieke identificatie van de autorisatie die aan een gebruiker toegekend kan worden. Hierbij mag het niet gaan om verzamelrollen.

*LET OP: indien er een naam van een groep gewijzigd wordt dan moet dit gecommuniceerd worden met LTB team FB/BV2. IMS ziet deze gewijzigde groep als een nieuwe groep waardoor we aanpassingen moeten doen om te zorgen dat de juiste autorisaties behouden blijven.

Account: Het account van de gebruiker in de applicatie. Deze is gelijk aan de gebruikersnaam zoals de gebruiker door IMS heeft toebedeeld gekregen in het gebruikersproces van LTB.

Lidmaatschap: het Account is lid van één of meerdere groepen, zodat de gebruiker van het account kan werken met de applicatie.

5.2 Applicatie beschikbaar maken in het LTB proces (formulieren)

Zoals eerder aangegeven heeft LTB team FB/BV2 een aantal gegevens nodig om de applicatie op te kunnen nemen in IMS. De gegevens die nodig zijn voor de inrichting kunnen met speciaal daarvoor opgestelde formulieren (formulier A, B of C) aan het team doorgegeven worden.

In Bijlage 1: Aanvraagformulieren vind je een beslisboom, zodat bepaald kan worden welk formulier nodig is, alsook de links naar de verschillende formulieren en de toelichting op de formulieren. De formulieren mogen alleen ingestuurd worden door applicatie eigenaren (product owners). Voor hulp of advies bij het invullen kan Functioneel Beheer Bedrijfsvoering team 2 benaderd worden. Er kan bijvoorbeeld een intake gepland worden om alles rondom het beschikbaar maken van de applicatie te bespreken. Compleet ingevulde formulieren worden afhankelijk van het formulier ingediend via RFF of gestuurd naar de EUM-LTB_Postbus.

Na ontvangst van het formulier beoordeelt Functioneel Beheer Bedrijfsvoering team 2 of er nadere afstemming nodig is. Indien alles duidelijk is wordt het formulier verwerkt en worden de permissies aangemaakt in IMS. Functioneel Beheer BV2 stelt vervolgens team Rollenbeheer LTB op de hoogte van de permissies en de informatie over het gebruik van de permissies. De rollenbeheerders stellen, na ontvangen van een opdracht via het contactformulier van de directies/proceseigenaren, de rollen samen in IMS. Vervolgens kunnen de managers deze rollen toewijzen aan de medewerkers. De eigenaar van de applicatie is zelf verantwoordelijk voor het informeren van de doelgroep over het gebruik van de applicatie.

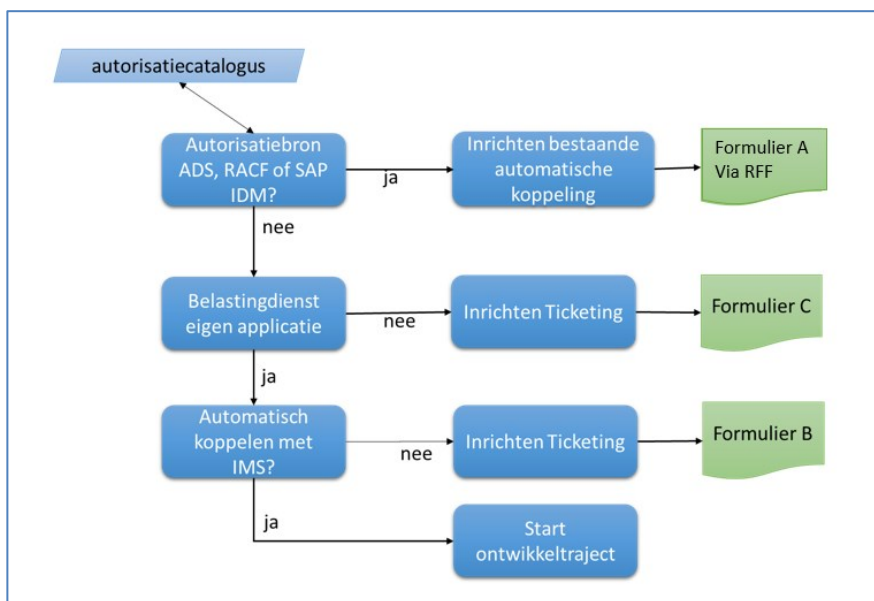
5.3 Checklist voor het aansluiten op IMS

Onderstaand een korte checklist betreffende het aansluiten op IMS. Tussen haakjes staat aangegeven in welk hoofdstuk je meer informatie kunt vinden over het betreffende punt.

- ☐ LTB, FB/BV2 (tijdig) betrokken bij de ontwikkelingen (5.1).
- ☐ Inrichting afgestemd met LTB, FB/BV2 (5.1).
- ☐ Autorisatiematrix opgesteld (4.2.1).
- ☐ Autorisatie informatie (IST) aangeleverd (5.1.1 en 5.1.2 en 5.1.3).
- ☐ Juiste formulier ingevuld, eventueel met hulp/advies van LTB, FB/BV2 (5.2).
- ☐ Compleet ingevulde formulier aangeleverd bij LTB, FB/BV2 (5.2).
- ☐ Terugkoppeling van LTB, FB/BV2 dat het formulier verwerkt is (5.2).
- ☐ De eigenaar van de applicatie heeft de doelgroep geïnformeerd (5.2).

6 Bijlage 1: Aanvraagformulieren

Met behulp van onderstaande beslisboom kun je een keuze maken, welk formulier er ingevuld en aangeleverd moet worden om de inrichting van het LTB-proces te starten.



Formulier A is voortaan alleen nog beschikbaar in ITSM en kan alleen nog maar via RFF ingediend worden. De overige formulieren worden uiteindelijk ook overgezet naar RFF.



Raadpleeg voor meer informatie de [Handleiding ITSM](#).

De overige formulieren (B en C) verstuur je voorlopig nog naar de [EUM-LTB postbus](#).

Alleen de applicatie eigenaren (productowners) mogen het formulier insturen. Dit is nodig om 1 aanspreekpunt te hebben waarmee afgestemd kan worden hoe de autorisatie in het LTB proces opgenomen moet worden.

Link naar de formulieren:

[Formulier A --> via ITSM](#)

[Formulier B](#)

[Formulier C](#)

[Toelichting op de formulieren](#)

7 Bijlage 2: Indeling csv-bestand voor IST informatie.

Aanleveren bestand

Minimale gegevens die aangeleverd moeten worden in het IST bestand:

- UserID (account)
- Groep

Het IST bestand dient consistent te zijn;

- Alle leden van een groep dienen ook als account aangeleverd te worden in hetzelfde bestand.
- Als een account wordt aangeleverd, dat geen lid is van een groep, dan zal dit account automatisch worden gedisabled binnen IMS.
- Groep dient ook aangeleverd te worden, als deze geen lidmaatschappen heeft.

Bestand informatie:

- *1 bestand van het formaat TXT of CSV, ; (punt-komma) als scheidingsteken*
- *inhoud is ruwe onbewerkte data uit de autorisatiebron*
- *Een volledig extract, geen delta t.o.v. vorige keer*
- *Frequentie 1x per week*
- *Er dienen geen quotes om waarden heen te staan. Tevens mogen er geen komma's, puntkomma's en diakrieten in de attributen staan.*
- *Het bestand dient bij elke aanlevering telkens hetzelfde formaat/indeling te hebben zodat deze automatisch kan worden verwerkt in IMS.*

8 Bijlage 3 : Afkortingen

Afkorting	Definitie
HBB	Handboek Beveiliging Belastingdienst
IMS	Identity Management System
IAM	Identity and Access Management
LTB	Logisch Toegangsbeheer Het geheel van organisatorische, technische en procesmatige maatregelen voor het verlenen van gecontroleerde toegang tot doelsystemen. LTB binnen de Belastingdienst wordt aangeduid als het LTB-proces. Overigens, Logisch Toegangsbeheer (LTB) realiseert Logische ToegangsBeveiliging (ook aangeduid als LTB).
RBAC	Role Based Access Control Rolgebaseerd autoriseren wordt in het vakgebied aangeduid met RBAC, Role Based Access Control.
SOD	Segregation Of Duties, oftewel scheiding van taken (functiescheidingen)
FUN	Functionele UserNaam of functioneel account
TPU	Tijdelijke Persoonlijke Usernaam
PU	Persoonlijke Usernaam

9 Bijlage 4 : Begrippen en definitie

Begrip	Definitie
Account	Een ICT-voorziening waarmee een gebruiker zich identificeert in een doelsysteem. Doorgaans kan een gebruiker een account pas gebruiken na authenticatie. Binnen de Belastingdienst worden voor alle accounts van één gebruiker over alle doelsystemen heen dezelfde gebruikersnaam gehanteerd (op enkele uitzonderingen na).
Applicatie	De functionele benaming van een ICT systeem, zoals het zich presenteert naar de gebruiker op het scherm en in de gebruikershandleidingen.
Applicatierol	Een verzameling van rechten in een applicatie die samen een bij elkaar behorend werkpakket vormt. In een applicatie geldt tussen de applicatierollen onderling het principe van functiescheiding. Voorbeelden zijn 'BVR – Raadplegen Ondernemingen', 'MS Access - Run-time' en 'SAP-TIJD – Goedkeurder'.
Authenticatieproces	Het proces richt zich op het uitvoeren en beheren van authenticatiemiddelen (wachtwoorden, tokens e.d.)
Authenticeren	Het bewijzen dat een gebruiker die zich toegang wil verschaffen ook degene is die als zodanig bij het doelsysteem geregistreerd is. Dit bewijzen kan op meerdere manieren, bijvoorbeeld via een wachtwoord of via een token.
Autorisatiebron	Systeem of applicatie waarmee een gebruiker specifieke rechten krijgt voor een applicatie.
Autorisatiematrix	Overzicht van de functionele autorisaties met bijbehorende technische autorisatie die beschikbaar zijn in een applicatie.
Autorisatieproces	Het proces richt zich op het toekennen van autorisaties en gebruikersrechten aan gebruikers van de informatiesystemen. Omgekeerd, als een identiteit door vooraf gedefinieerde regels geen toegang meer mag hebben op bepaalde informatie binnen informatiesystemen, zal deze automatisch worden ontnomen.
(Bedrijfs)rol	Representatie van een verzameling van werkzaamheden en bijbehorende permissies, die veelal als een geheel wordt toegewezen aan een bepaald type functionaris. De rol kan samengesteld zijn uit één of meer procesrollen. Omdat het LTB-proces is ingericht volgens het RBAC-principe, krijgen gebruikers alleen rollen en/of bijzondere taken direct toegewezen. Permissies worden niet direct toegewezen maar worden afgeleid.

Functioneel Beheer BV2	Functionaris(sen) die het functioneel beheer voer(en)t over de applicaties welke het LTB-proces ondersteunen. (o.a. IMS, B2W). Zij zijn gepositioneerd in de organisatie onder SSO F&MI afdeling LTB en FB/BV
Geautomatiseerde rol	Rol welke automatisch o.b.v. SAP-HR gegevens toegewezen kan worden aan gebruikers.
Gebruiker	Een gebruiker is in zijn basisvorm de representant van een natuurlijk persoon, die toegang nodig heeft tot de geautomatiseerde systemen van de Belastingdienst.
Gegevenstoegang	Een vorm van permissie waarbij het geen applicatierol betreft, maar toegangsrechten (muteren of alleen lezen) voor elektronische gegevens. Voorbeelden zijn de PcNu samenwerkingsgebieden (met collega's delen van MS Office documenten in de Windows omgeving) en IBM Notes Teamrooms.
Groep	De technische benaming van een autorisatie, de technische representatie in doelsystemen van applicatierollen of toegangsrechten. Het is een unieke identificatie van de autorisatie die aan de gebruiker kan worden toegekend.
Identificatieproces	Het proces richt zich op het administreren en beheren van identiteiten van gebruikers.
IST	De feitelijk aanwezige accounts en ICT-autorisaties in de doelsystemen. Dit is op een zodanig niveau, dat de IST te vergelijken is met de SOLL.
Niet-geautomatiseerde rol	Rol welke handmatig door de leidinggevende toegewezen wordt aan een gebruiker.
Permissie	Verzamelbegrip voor zowel de functionele aanduidingen applicatierol als de gegevenstoegang. Permissies geven inhoud aan rollen en bijzondere taken.
Persona	Extra userID voor een gebruiker, altijd gekoppeld aan het eigen UserID van de gebruiker (aan de hoofdentiteit).
Risicogroep	identificatie van de groep medewerkers welke het soort risico van de roltoewijzing kunnen fiatteren.
Rol	Een rol is een zodanige groep van functioneel bij elkaar behorende rechten, taken, transacties of commando's dat er binnen deze rol (en ten opzichte van andere rollen) uit eisen van functiescheiding geen onverenigbare autorisatie kunnen ontstaan. (UBGI = uitvoeren, beoordelen goedkeuren en informeren) (RASCI = responsible, accountable, supportive, consulted en informed)