



DBO Aansluitvoorwaarden voor Applicaties

De binnen DBO aangeboden- en te gebruiken applicaties dienen te voldoen aan het Rijkskader vanuit CIO Rijk, **IDWOR beleidskader 8 werkplekafhankelijkheid van klantapplicaties** (zie bijlage)

Daarnaast dient aan onderstaande aansluitvoorwaarden te worden voldaan:

NB. De aansluitvoorwaarden zullen periodiek worden beschouwd en waar nodig aangepast.

Aansluitvoorwaarden

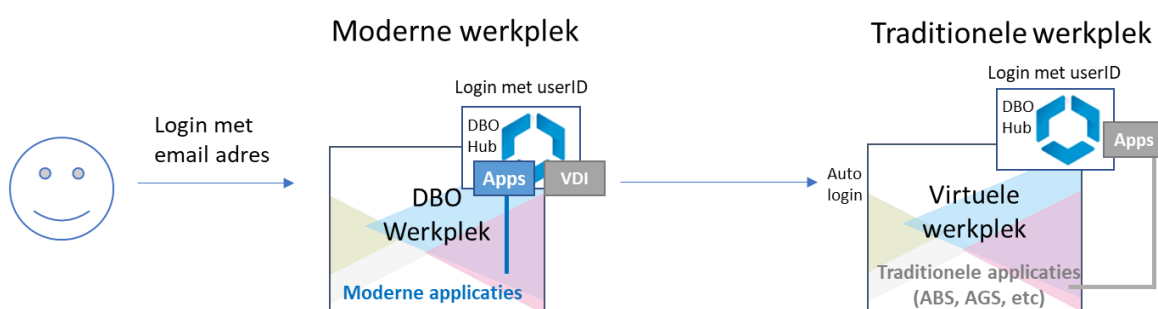
- Geen afhankelijkheid met versies van het Operating systeem (windows 10, macOS, iOS of Android).
- M.a.w. de updates van het OS mogen geen invloed hebben op de werking van de applicatie

Browser

- Geen afhankelijkheid van een specifieke (versie van) een Browser. De applicatie moet met iedere (versie van) een browser overweg kunnen. Zowel op een Windows of een MAC-device, alsook op een mobile device (smartphone of tablet)
- De webgebaseerde applicatie dient altijd HTTPS te gebruiken
- Authenticatie van de eindgebruiker in de applicatie dient middels SAML2 authenticatieprotocol te geschieden

Windows

Er zijn primair twee plaatsen waar Windows applicaties aangeboden kunnen worden:



Met DBO wordt het mogelijk om met moderne applicaties en cloud diensten te werken.

Moderne applicaties zijn applicaties die fysiek op de werkplek komen zoals dat op smartphones en iPads gebeurt. Dat betekent dat de applicaties via internet automatisch van updates worden voorzien, dat de applicaties hun eigen beveiliging regelen (conform [het Zero Trust model](#)), dat geen gebruik wordt gemaakt van verouderde technieken (zoals bijvoorbeeld de N: en de Q: schijf), en dat er geen technische afhankelijkheden zijn met (versies van) componenten die op de werkplek staan (runtimes, drivers). Voorbeelden van moderne applicaties zijn de Chrome browser, de Office applicaties en de Intelligent Hub. Ook een deel van de eigen Belastingdienst web applicaties is nu reeds geschikt om op een moderne manier te gebruiken.



Veel Belastingdienst applicaties zijn echter nog **traditionele applicaties**.

Deze zijn gebouwd in de tijd dat de beveiliging anders ingericht was: niet de applicatie zelf maar de omgeving van de applicatie werd beveiligd en afgeschermd van de buitenwereld. Dat werd gerealiseerd door de werkplekken te laten draaien binnen het interne Belastingdienst netwerk, waardoor ze bijvoorbeeld de N: en Q: schijf konden gebruiken. Ook konden de werkplekken volledig onder eigen beheer worden gehouden omdat het aantal updates relatief gering was, de DWB werkplek en alle versies van de componenten volledig in beheer waren en dat de enige “landingsplaats” van applicaties was.

De modernisatie van traditionele applicaties loopt reeds enkele jaren, maar is nog niet afgerond. En omdat we van moderne diensten zoals Office365 gebruik willen maken, is het zaak dat we binnen DBO zowel moderne als traditionele applicaties ondersteunen. Dat doen we op de volgende manier:

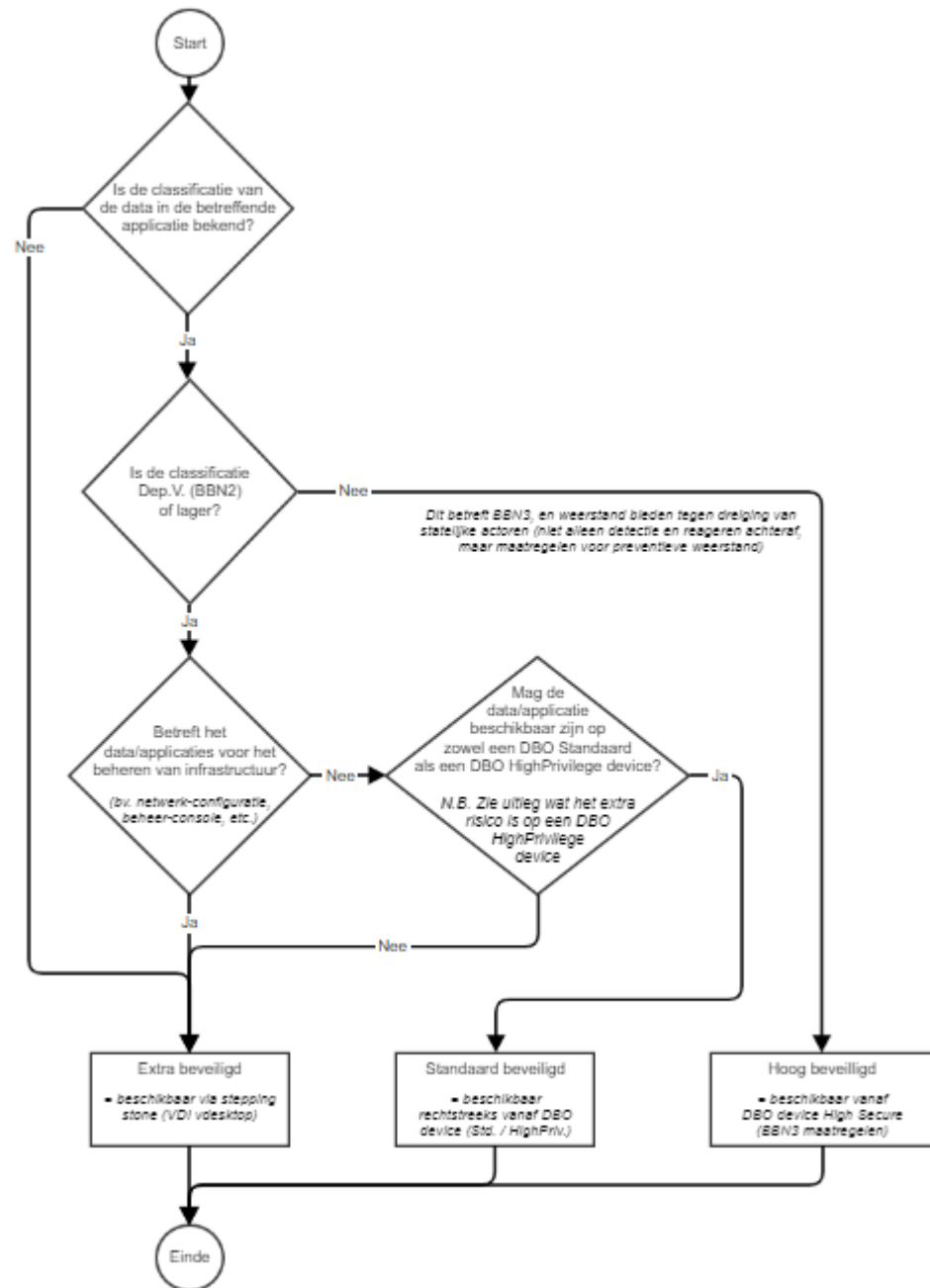
- Op de fysieke DBO werkplek staan de moderne applicaties
- Op een DBO werkplek kan ook een virtuele werkplek worden gestart, deze virtuele werkplek draait volledig binnen het interne Belastingdienst netwerk, daarom kunnen op deze virtuele werkplek alle traditionele applicaties worden gebruikt.

In onderstaande tabel staan voorbeelden wat je op een DBO werkplek kunt verwachten.

<u>Moderne Werkplek op de fysieke DBO werkplek</u>	<u>Traditionele Werkplek op de virtuele werkplek</u>
Moderne applicaties	Traditionele applicaties (ABS, AGS, enzovoort)
MS Word, Excel, PowerPoint	MS Word, Excel, PowerPoint
MS Outlook, Teams, OneDrive	MS Outlook, Teams (geen video), OneDrive <i>online</i>
Toegang tot cloud diensten, bijvoorbeeld M365	Geen toegang tot cloud diensten
Notes mail (Verse Web) als archief	Notes mail (Verse Web) als archief
<i>Geen</i> toegang tot N:\ en Q:\	Toegang tot N:\ en Q:\
Printen via print-to-mail	Printen op kantoor printer (MFP)
Open internet	Gefilterd internet (Internet op de werkplek)
Applicaties via het startmenu en de Hub	Applicaties via startmenu en de Hub
Applicaties installeren via Appstore	Niet mogelijk om zelf applicaties te installeren

Naar aanleiding hiervan, de volgende aansluitvoorwaarden:

- Voor installatie op een Fysieke Windows werkplek geldt: De applicatie
 - moet geïnstalleerd kunnen worden middels VMware Workspace One
 - heeft geen afhankelijkheid van de Windows versie i.v.m. Windows auto-update
 - heeft geen afhankelijkheid van (specifieke versies van) componenten op de werkplek (runtimes en drivers) daar deze automatisch geupdate worden
 - heeft geen harde afhankelijkheid met de versie van de server/data in het datacenter in een client server architectuur
 - heeft geen data op Q: of N: nodig, daar deze drives *niet* beschikbaar zijn op een fysieke Windows DBO werkplek
 - dient de eigen beveiliging te regelen voor data en applicatie in een zero trust omgeving. De eigenaar van de applicatie en data dient goedkeuring te geven voor het beschikbaar stellen van de applicatie op een DBO Windows werkplek. Indien dit niet het geval is zal de applicatie aangeboden via een Virtuele DBO werkplek. Het beslisschema hiervoor is hieronder ingevoegd:



Figuur: Beslisflow voor applicaties op een DBO werkplek

- Voor installatie op een virtuele Windows werkplek (Datacenter werkplek) geldt:
 - installeerbaar op Windows, als VMware Appvolume, of als VMware Thinapp
 - de reeds geldende aansluitvoorwaarden voor VMware AppVolumes gelden ook hier
- Installeren van de applicatie moet geautomatiseerd kunnen worden om de gebruiker niet lastig te hoeven vallen met de installatie



macOS

- De applicatie moet geïnstalleerd kunnen worden middels VMware Workspace One
- Installeren van de applicatie moet geautomatiseerd kunnen worden om de gebruiker niet lastig te hoeven vallen met de installatie

IOS en Android

Link: <https://confluence.belastingdienst.nl/pages/viewpage.action?pageId=462924058>

1.	Distributie	De App moet geïnstalleerd kunnen worden middels VMware Workspace One.
2.	Administratie	Voor het beschikbaar stellen van de app is een volledig ingevuld intake formulier noodzakelijk.
3.	Configuratie van de App moet uitgevoerd kunnen worden met App Config	Om het gebruik van de Apps voor de gebruiker zo eenvoudig mogelijk te maken, moeten instellingen met App Config voor geconfigureerd kunnen worden. Voorbeelden: servernaam, poortnummer van de Backend.
4.	Op de App wordt een actief onderhoud en update-beleid toegepast.	Dit houdt in dat de App tegen het beta-programma van iOS en/of Android getest wordt. Eventuele problemen met een toekomstige OS-release zijn in 90% van de gevallen opgelost bij het uitkomen van de OS-release. En in 10% van de gevallen binnen een week na de release.
5.	Configuratie volgens geldende beveiligingseisen	De App moet geconfigureerd kunnen worden zodat deze voldoet aan de beveiligingseisen zoals gesteld aan de rijksoverheid. (BIO, CIS-baseline).
6.	Toekenning applicaties	Toekenning (en verwijderen) van een applicatie verloopt via een groepslidmaatschap in de AD/IMS. De IMS groep dient door de aanvrager te worden ingericht, voordat het configuratie-item wordt aangeleverd.
7.	Inrichting en beheer backend services	De technisch eigenaar van de App is ook verantwoordelijk voor het inrichten en beheren van de backend service die bij de app hoort.
8.	Ontsluiting van Backend (App alleen voor intern gebruik)	Ontsluiting van backend moet via WS1 (Tunnel) indien de App alleen voor intern gebruik is bedoeld (alle eindgebruikers van de App zijn aangemeld bij WS1).



9.	Ontsluiting van Backend (App voor intern en extern gebruik)	Ontsluiting van backend moet via WS1 (Tunnel) voor intern gebruik (Belastingdienst medewerkers). Indien een App (ook) voor extern gebruik is bedoeld dan moet gebruik worden gemaakt van MAM (Mobile Application Management) (beschikbaar vanaf Q3 2022?) Alternatieve ontsluiting van een backend door een App voor extern gebruik is via de Webservices Gateway (Datapower). Hiervoor hoeven de gebruikers niet geautoriseerd worden binnen WS1. De Webservice Gateway heeft een eigen set van aansluitvoorwaarden.
10.	Apps en publieke Clouddiensten	Apps die gebruik maken van publieke clouddiensten moeten voldoen aan "beleid publieke clouddiensten versie 1.0". Apps die gebruik maken van publieke clouddiensten moeten vooraf getoetst worden door de Cloud-toetsingscommissie. Apps die gebruik maken van publieke clouddiensten mogen geen toegang hebben tot gegevens met classificatie BBN2 en BBN3.
11.	Apple Business Manager – VPP	Apps die via Apple Business Manager – VPP (Volume Purchase Plan) gekocht kunnen worden hebben een Pré (Voor zowel Licentiebeheer als het kunnen installeren zonder Apple-ID).
12.	Attack en Penetration Test (A&P test)	Apps die een verbinding maken met de Belastingdienst Infrastructuur (Backend-service) moeten voor in productie name een A&P test hebben ondergaan. Dit is een verantwoordelijkheid van de technisch eigenaar van de App.
13.	Licentiekosten	Indien een app voor zakelijk gebruik licentiekosten met zich meebrengt, dan dient dit met budget te zijn afgedekt door de technisch eigenaar van de app.
14.	No password policy	Indien mogelijk dient SSO te worden geïmplementeerd. Naast configuratie binnen Workspace ONE moet dit voor de te ontsluiten Back-



		end worden ingeregeld (door de technisch eigenaar van het back-end systeem).
15.	Documentatie en ondersteuning	Documentatie (handleiding, instructies, gebruikerskaart) en ondersteuning (Service Desk) moet zijn ingericht voorafgaand aan de implementatie van de App.
16.	Problem en Incident proces	Voor zowel de app als een eventueel bijbehorende backend is het Problem en Incident proces ingericht.



Bijlage:

Uitwerking beleidskader 8 werkplekonafhankelijkheid van klantapplicaties

Inleiding

Programma Interoperabiliteitskaders Digitale Werkomgevingen & Rijkskantoren (IDWOR) is ingericht om de samenwerking in rijkskantoren en tussen dienstverleners te verbeteren. Hierdoor wordt samenwerking tussen medewerkers eenvoudiger, evenals tijd, plaats en apparaatonafhankelijk werken (TPAW). IDWOR volgt een groeimodel waarin in de loop van de tijd individuele kaders worden vastgesteld. Dit document beschrijft het achtste kader.

Dit kader gaat in op het moment dat het door het CIO beraad is vastgesteld. Verantwoordelijkheid voor het beheer van dit kader, evenals voor IDWOR als geheel, ligt bij de directie CIO Rijk van BZK.

Doel & oplossing

Naar aanleiding van de memo Groen/Barendse¹, waarin gepleit wordt om harde eisen te stellen aan de werkplekonafhankelijkheid van klantapplicaties, is dit kader tot stand gekomen.

Met 'werkplek' wordt hier een fysiek of virtueel apparaat voor de eindgebruiker bedoeld wat de gebruiker in staat stelt om conform het EAR-principe: Plaats-Tijd- Organisatie- Apparatuuraafhankelijk te werken.

Waar in de memo Groen/Barendse vooral wordt ingezet op updates (en upgrades) van Windows is het van belang om expliciet te benadrukken dat de in dit kader vastgelegde afspraken ook van toepassing zijn op:

- alle koppelvlakken/koppelingen en integraties met de werkplek (plugins, extensions, middleware en frameworks) zoals Flash, Silverlight, Java, DotNet, maar ook koppelingen met Outlook, Excel of Word die een werkplekcomponent nodig hebben en dus potentieel problemen kunnen veroorzaken;
- andere verschijningsvormen die applicaties kunnen hebben ("the three screens")
 - Windows/MacBook client applicatie (fatclient screen)
 - Web applicatie (web screen)
 - Mobile app (mobile screen)

¹ "Memo next steps rationalisatie ICT-landschap def"



Afspraken

Om ervoor te zorgen dat er zoveel mogelijk software ontwikkeld wordt die browser-² en werkplekonafhankelijk werkt, worden onderstaande afspraken gemaakt. Wanneer van deze afspraken moet worden afgeweken, gebeurt dit uitsluitend na overleg met CIO Rijk.

- Buiten een 'moderne browser'³ mag er **geen andere afhankelijkheid** van de werkplek zijn, met andere woorden de updates van de werkplek mogen geen invloed hebben op de werking van de applicatie;
- Webapplicaties functioneren onafhankelijk van de gekozen browser met ondersteuning voor de in de markt gangbare browsers, zoals: Chrome, Edge en Firefox.
Hierbij mag er ook geen afhankelijkheid zijn met een specifieke versie van een browser. De applicatie moet met iedere recente⁴ versie van een moderne browser overweg kunnen. Zowel op een Windows of een MAC-device, alsook op een mobile device (smartphone of tablet). Moderne browsers worden in een hoog tempo doorontwikkeld: ook daarop moet de webapplicatie permanent worden bijgehouden om te blijven voldoen aan deze laatste standaarden.
- Een applicatie heeft geen harde afhankelijkheid met andere applicaties in- of op het device, koppelingen met andere applicatie(componenten) dient te geschieden op basis van open standaarden en moeten plaatsvinden vanuit het backend op basis van gedefinieerde API's. Een voorbeeld ter verduidelijking: de Exchange-koppeling niet realiseren met een plugin voor Outlook op de werkplek, maar via EWS met de Exchangeserver.
- Applicatieverkeer dient versleuteld te zijn (bv. HTTPS, TLS1.2/1.3)
- Er moet verplicht gebruik worden gemaakt van relevante (open) standaarden, gemakshalve wordt verwezen naar de lijst met open standaarden van het Forum Standaardisatie ([Lijst open standaarden | Forum Standaardisatie](#)) en de webstandaarden die zijn gedefinieerd door het W3C (<https://www.w3.org/standards/>) en de IETF (<https://www.ietf.org/standards/>).
- SSoN geschied via het moderne authenticatie protocol [SAML2](#) (rijksbreed de federatieve standaard), autorisatie (voor toegang tot resources) via [Oauth](#).

Overgangsregeling

Dit kader probeert niet te bewerkstelligen dat alle applicaties die extra componenten (plugins, extensions, middleware en frameworks) op de werkplek nodig hebben direct worden herschreven naar webapplicaties. Bij aanschaf of

² Volledige browser-onafhankelijkheid is (nog) niet mogelijk omdat de moderne standaarden niet in dezelfde mate en/of hetzelfde tempo worden ondersteund door alle webbrowsers.

³ Definitie 'moderne browser': een browser die maximaal met de moderne webstandaarden als genoemd onder de 5e bullet om kan gaan.

⁴ Definitie 'recent': volgens het n/n-1-stramien: huidige (n) of vorige (n-1) hoofdversie.



bouw van nieuwe software of bij vernieuwbouw van bestaande systemen dient dit kader te worden gehanteerd.

Het voldoen aan dit kader moet voor de eigenaren van applicaties onderdeel gaan worden van hun LCM-agenda op de applicaties, waarbij/waardoor de overgang planbaar wordt.