# Aansluitvoorwaarden generieke infrastructuur UWV

## 1. UWV infrastructuur leveranciers en diensten in de komende jaren 2022-2024

De UWV infrastructuur, bestaande uit werkplek, netwerk, security en IAM diensten, wordt momenteel (juni 2021) grotendeels geleverd door KPN. In verband met aanbestedingen komen opvolgende leveranciers in de periode 2023-2024 in beeld zodra betreffende diensten in die periode worden gegund. In dit document is daarom sprake van KPN en/of opvolgende leveranciers (hierna te noemen **KPN e.a.**).

De hosting - en technisch applicatiebeheerdiensten voor bedrijfsapplicaties worden geleverd door DXC. Deze situatie wijzigt de komende jaren niet.

In dit document is, in verband met aanbestedingen en daarmee gepaard gaande veranderingen, in de diensten in sommige gevallen sprake van 3 situaties:

- CMO: Current mode of Operation: De status van de diensten tot uiterlijk het einde van de huidige contractperiode, zijnde 31-12-2023.
- TMO: Transition mode of Operation: De hybride status van de diensten gedurende de transitie van huidig contract naar nieuwe contracten, in de periode 2023 tot en met eind 2024.
- FMO: Future mode of Operation: De status van de diensten na afloop van de aan de aanbestedingen gerelateerde transitie. De FMO van de diensten wordt in het jaar 2024 bereikt, uiterlijk 31-12-2024.

## 2. Aansluitvoorwaarden netwerk UWV

Hieronder worden de koppelvlakken die van toepassing zijn bij het aansluiten van een nieuwe ICT dienst op het UWV netwerk beschreven. Opdrachtnemer dient zich te conformeren aan de beschreven koppelvlakken en toegangsbeveiliging.

### LAN/WLAN

*Koppelvlak (W)LAN - CMO*

- Het LAN van UWV biedt - in alle locaties van UWV - 1 Gbps RJ45 aansluitingen voor aan te sluiten devices. Devices worden via de aanwezige CAT 6+ gebouwbekabeling aangesloten.
- Het LAN van UWV is gesegmenteerd op basis van VLAN's, voor werkplekken (zgn. trusted LAN) en diverse doelgroep netwerken van overige (ICT, facilitaire- en beveiligings) devices.
- Tevens is in alle locaties Wireless LAN (WLAN) aanwezig. Het WLAN is gesegmenteerd naar doelgroepen: Besloten trusted / govroam voor internet toegang voor medewerker overheid / openbaar hotspot voor gasten.
- Het LAN en trusted WLAN van UWV gebruiken 802.1x toegangsbeveiliging. Devices dienen zich te authentiseren met een certificaat. Indien dit niet mogelijk is, geldt een geregistreerd MAC adres als authenticatiemiddel. Niet geauthentiseerde devices en eigen devices hebben geen toegang tot het LAN en trusted WLAN.
- Op het LAN is QoS ingericht. VOIP en video vallen onder de real time klasse "platinum".
- Het LAN ondersteunt Power over Ethernet.
- Het WLAN ondersteunt 2,4 GHz en 5 GHz netwerkfrequenties.
- Voor locatie-gebonden devices van Opdrachtnemer is op aanvraag een IPv4 subnet beschikbaar (doelgroepen netwerk LAN).
- IPv6 wordt op het interne netwerk niet ondersteunt.
- Het LAN en WLAN van een locatie hebben geen directe koppeling met het internet of andere externe netwerken of ICT diensten. Al het verkeer loopt via het MPLS WAN en

een centrale koppeldienst met gestapelde securityfuncties (w.o. firewalls), alwaar Internet, datacenters en partner netwerken gekoppeld zijn.

*Koppelvlak (W)LAN – FMO: Belangrijkste verschillen met CMO:*

- WLAN govroam is het primaire wifi netwerk voor UWV gebruikers. Authenticatie op basis van 802.1x certificaat of UID/PW, conform richtlijnen govroam. Een trusted besloten WLAN bestaat niet meer.
- Ongeauthenticeerde devices / gebruikers hebben toegang tot een hotspot WLAN, mogelijk op basis van een door selfservice verkregen ticket.
- Het WLAN ondersteunt (en is ingemeten op) voice en video
- Het (W)LAN is functioneel gekoppeld aan een lokale internet breakout maar voor specifieke toepassing ook aan een besloten bedrijfsnetwerk, op basis van SD-WAN en applicatie based routing
- Het (W)LAN biedt zo direct mogelijke connectiviteit naar op Internet bereikbare SAAS en cloud diensten waarvoor lage latency en hoge bandbreedte een vereiste is. Video, Voice, Webrtc sessies worden dus zo snel mogelijk geoffload naar internet
- IPv6 is, indien IP V4 niet mogelijk is, op het interne netwerk beschikbaar

*Koppelvlak (W)LAN - TMO:*

- Gedurende TMO worden lokaties voorzien van een nieuw LAN/WLAN en WAN, grotendeels Software defined, conform de FMO beschrijving. Er zal sprake zijn van een mix van locaties met LAN/WAN – CMO en LAN/WAN – FMO. CMO en FMO LANs zullen onderling bereikbaar zijn.

**WAN**

*Koppelvlak WAN - CMO:*

- Het datacenter van Opdrachtnemer kan desgewenst gekoppeld worden aan het netwerk van UWV via een door UWV te leveren WAN aansluiting
- Het WAN van UWV biedt diverse aansluitingsprofielen:
    - Redundante twin datacenter aansluitingen (beschikbaarheid 99,99%)
    - Redundante WAN aansluiting (beschikbaarheid 99,95%)
    - Enkelvoudige WAN aansluiting (beschikbaarheid 99,85%)
- Voor een glas verbinding geldt de volgende leverbare bandbreedtes: 20mb, 30mb, 50mb, 80mb, 100mb, 200mb, 300mb, 500mb, 800mb, 1Gb. 10Gb.
- Levering van een nieuwe aansluiting duurt maximaal 16 weken indien de aan te sluiten locatie al op KPN glas is aangesloten. Als de locatie niet op KPN glas is aangesloten is de doorlooptijd 18-21 weken vanwege de afhankelijkheid van de regionale ligging en vergunning traject bij de gemeente.
- Op de segmenten (MPLS VRF's) in het WAN wordt prioritering op basis van QoS/CoS ondersteund.
- Het WAN is functioneel ingedeeld in Trusted/Gast/Facilitair/Beheer, de verkeersstromen worden in overleg met de betreffende architecten en productmanagers van UWV en KPN e.a. toegewezen. Locaties zijn onderling bereikbaar per functie.
- De WAN aansluiting van een locatie of datacenter heeft geen directe koppeling met het internet of andere externe netwerken of ICT diensten. Al het verkeer loopt via het MPLS WAN en een centrale koppeldienst met gestapelde securityfuncties (w.o. firewalls), alwaar Internet, datacenters van ICT leveranciers en partner netwerken gekoppeld zijn.
- Het is desgewenst mogelijk een IPSEC VPN koppeling tussen UWV en een SAAS dienst te realiseren.

*Koppelvlak WAN - FMO: Belangrijkste verschillen met CMO:*

- Het WAN van UWV is een software defined netwerk. Het belangrijkste onderliggend netwerk waar alle lokaties en datacenters op aangesloten zijn is Internet. Daarnaast zullen er mogelijk nog private WAN verbindingen gebruikt worden
- Het WAN ondersteunt toegang tot internet, tot clouddiensten en tot datacenters van aangesloten leveranciers.
- Indien een locatie van Opdrachtnemer wordt aangesloten, wordt de betreffende locatie voorzien van een SDWAN device. Dit device bepaalt de functionaliteit en connectiviteit van de betreffende locatie en zorgt voor de noodzakelijke afscherming en beveiliging, in combinatie met in het netwerk van UWV aanwezige firewall functies.
- Levering van een aansluiting van een nieuwe locatie kent een kortere doorlooptijd dan de CMO situatie.
- Het WAN maakt gebruikt van software defined centrale beveiligings-, routerings- en prioriteringsmechanismes. In overleg met Opdrachtnemer worden de beveiligings- en kwaliteitsparameters voor de aansluiting met Opdrachtnemer vastgesteld.
- Het WAN kan nog steeds functioneel ingedeeld zijn in bijvoorbeeld Trusted/Gast/Facilitair/Beheer, maar deze indeling kan in FMO sterk afwijken van de CMO situatie. De verkeersstromen worden in overleg met de betreffende architecten en productmanagers van UWV en KPN e.a. toegewezen. Locaties zijn onderling bereikbaar.

*Koppelvlak WAN - TMO:*
- Gedurende TMO worden lokaties voorzien van een nieuw LAN/WLAN en SD-WAN, grotendeels Software defined, conform de FMO beschrijvingen. Er zal sprake zijn van een mix van locaties met WAN – CMO en SD-WAN – FMO. CMO en FMO lokaties zullen onderling bereikbaar zijn.

**UWV Koppeldienst (UKD)**

*Koppelvlak firewall UWV Koppeldienst (UKD) - CMO*
- Alle door 3de partijen aan UWV geleverde ICT diensten worden via de UWV koppeldienst op veilige wijze gekoppeld met het UWV netwerk en daarop aangesloten werkplekken.
- Indien de ICT dienst vanuit het datacenter van Opdrachtnemer geleverd wordt, dan is een externe WAN/VPN koppeling van toepassing (zie koppelvlak internet/externe koppeling). Er zal - voorafgaand aan de realisatie - door KPN en in samenspraak met Opdrachtnemer, een ontwerp gemaakt worden. In het ontwerp worden aspecten zoals IP subnet, adresvertaling, type WAN aansluiting en redundantie meegenomen.
- Indien de ICT dienst van Opdrachtnemer op basis van housing/colocation of hosting diensten worden aangeboden aan UWV, dan is het koppelvlak met UWV niet standaard beschikbaar. Er moet gebruikt gemaakt worden van de DXC datacenter dienst. Er zal voorafgaand aan de realisatie door DXC een ontwerp gemaakt worden, in samenspraak met Opdrachtnemer en KPN. Het DXC datacenter is gekoppeld aan het UWV netwerk, dus ontsluiting van de applicatie richting UWV gebruikers is na realisatie van de hosting/housing als vanzelf geregeld.
- Indien de ICT dienst van opdrachtnemer vanuit een SAAS omgeving op internet wordt aangeboden, wordt standaard gebruikt gemaakt van het internet koppelvlak op de UKD dienst. Standaard koppelvlak is HTTPS. De UWV gebruikers benaderen de SAAS oplossing via een forward proxy.
- Binnen de UKD firewall wordt QOS niet ondersteunt.
- Firewall policies gaan altijd uit van dicht-tenzij: Er worden alleen de strikt noodzakelijke specifieke IP adressen/subnetten en poorten opengesteld.
- Het is mogelijk om realtime (media) verkeer via een high bandwidth internet verbinding te routeren van/naar bv een SAAS dienst.

*Koppelvlak firewall UWV Koppeldienst (UKD) – FMO*

- De UWV koppeldienst in de FMO situatie biedt dezelfde functionaliteit als de CMO
- De security diensten zullen echter deels omgebouwd zijn naar een Secure Web gateway // CASB / SDP set van functies, ten behoeve van ICT diensten die als SAAS of cloud dienst worden aangeboden.
- Daarnaast zal een on prem firewall voor de legacy diensten beschikbaar zijn als koppelvlak.

**Active Directory**

*Koppelvlak Active Directory (CMO):*
- Alle gebruikers accounts, werkplekken van UWV maken deel uit van het KA Active Directory domein.
- Rollen worden geregistreerd in het Autorisatie Beheer Systeem (ABS), door UWV beheerd. Deze rollen worden automatisch geprovisioned naar de Active Directory autorisatiegroepen.
- Op de AD van UWV is het mogelijk om een trust relatie te maken met een resource domein, mits er sprake is van een WAN koppeling / betrouwbare verbinding.
- Op de AD van UWV is het mogelijk een LDAPS koppeling te realiseren, om users en rechtengroepen uit te lezen.
- Op de AD van UWV is het mogelijk een ADFS koppeling te realiseren, t.b.v. federatieve authenticatie en autorisatie.
- Ondersteunde authenticatieprotocollen zijn: Kerberos, SAML, Openid-Connect, WS-FED. Een autorisatiemodule van een applicatie kan ook LDAPS gebruiken.
- UWV streeft altijd naar Single Sign On, dat wil zeggen dat een op het KA domein ingelogde gebruiker automatisch wordt ingelogd op de bedrijfsapplicatie van Opdrachtnemer, mits de gebruiker de juiste autorisaties heeft voor deze applicatie

*Koppelvlak Active Directory TMO en FMO – belangrijkste verschillen met CMO*
- LDAP(S) wordt niet meer ondersteunt.
- De eventuele van belang zijnde attributen behorende bij een gebruiker kunnen via ABS of opvolgend identity en autorisatiebeheer systeem worden toegevoegd aan het AD gebruikersaccount
- Standaard authenticatie voorziening voor een applicatie (SAAS, hosted) wordt AD FS, UWV biedt daarvoor een IDP, deze is via internet bereikbaar.
- Opdrachtnemer zorgt voor de juiste Service Provider inrichting. Standaard protocollen zijn SAML 2.0 , OpenID-Connect, WS-FED.
- Tevens is het voor Opdrachtnemer van belang (en moet hier rekening mee houden) dat de Active Directory dienst van UWV meegroeit en integreert met alle ontwikkelingen geboden vanuit de Azure Active Directory functionaliteit.

**Koppelingen**

*Koppelvlak remote beheer:*
- Beheer op de UWV infrastructuur is mogelijk via een vaste koppeling (externe koppeling), via de Dienst Externe Toegang. De keuze en inrichting is hierbij afhankelijk van de contractuele basis en de aard van de werkzaamheden en daarom als maatwerk te ontwerpen. Bij voorkeur wordt RDP of HTTP(S) gebruikt.

Koppelvlak VOIP
- Voor het aansluiten van IP telefonie is een Session Border Controller dienst beschikbaar.
- De SBC dienst is een verbijzondering van de UKD specifiek voor IP telefonie diensten, typisch VOIP en IP-fax diensten. De SBC systemen zijn uitgerust met ieder 1.000 licenties t.b.v. 1.000 gelijktijdige kanalen verdeeld over twee datacenters. Het aantal fysieke Ethernet interfaces waarover dit verkeer afgewikkeld kan worden is per SBC beperkt tot 4.

- De volgende koppelvlakken zijn specifiek beschikbaar op de SBC dienst.
  OSI Laag 2
  - Protocol: GbE
  - RJ45 koper

  OSI Laag 3+4
  - TCP/IP
  - UDP

  OSI Laag 7
  - SIP
  - RTP
- IP telefonie krijgt op het netwerk voorrang door het gebruik van Quality of Service (klasse realtime).
- Een vast VOIP telefoontoestel moet ondersteuning bieden voor 802.1x. Dit protocol is op het gehele netwerk van toepassing.

**Werkplek**

*Koppelvlak werkplek (CMO):*
- Voor het ontsluiten van applicaties op de werkplek van UWV geldt een Windows Server 2016/Citrix terminal server architectuur. De werkplek van UWV is namelijk altijd een virtuele desktop en kan binnen en buiten UWV benaderd worden
- Applicatie ontsluiting is bij voorkeur op basis van Edge Chromium, zonder plug-ins, op basis van HTML 5.
- Indien zero footprint niet mogelijk is, biedt UWV de mogelijkheid plug-ins met App-V gevirtualiseerd aan te bieden. Indien webbased applicatieontsluiting niet mogelijk is, biedt UWV de mogelijkheid een applicatie-client met App-V gevirtualiseerd aan te bieden. Dit vereist wel een goedkeuring van de architecten van UWV
- Drivers voor randapparatuur zijn bij voorkeur Windows 10 logo gecertificeerd, en dienen aanvullend voor de UWV werkplek gecertificeerd te worden i.v.m. de beveiligingsmaatregelen op o.a. USB poorten.

*Koppelvlak werkplek (FMO):*
- De werkplek van UWV is een Windows 10 (of opvolgende versies) gebaseerde werkplek, vaak een laptop. De geboden basisfunctie is de M365 functionaliteit.
- Applicaties worden op basis van een browser benaderd en bediend.
- Legacy client/server applicaties worden / zijn geïnstalleerd op een Citrix omgeving en worden met een ICA client benaderd.
- Bij voorkeur worden applicaties niet rechtstreeks op de werkplek geïnstalleerd, maar verloopt dit op beheerste wijze door gebruik van een app store.
- Opdrachtnemer dient dus er voor te zorgen dat eventueel op de UWV werkplek benodigde applicaties een webbased interface bieden of te installeren zijn via een door Opdrachtnemer aangeboden installatiepackage, welk zal worden opgenomen in de UWV App Store.

**Beveiligde gebruikersinterface voor SAAS:**

Voor ontsluiting van SAAS applicaties op een standaard UWV Werkplek met actuele browser stelt de Opdrachtnemer een https interface beschikbaar..

Voor de https verbinding geldt dat er sprake dient te zijn van encryptie op de applicatielaag conform actuele beveiligingsrichtlijnen (momenteel minimaal TLS 1.2 en voorgeschreven cyphersuites) van het NCSC. Hierbij gelden de volgende voorwaarden:
- Het servercertificaat wordt uitgegeven door een door UWV gekozen CA. UWV vraagt dit certificaat aan.

- De te ontsluiten applicatie van inschrijver zal op basis van een uwv.nl URL - of een URL in een daaronder vallend specifiek subdomein - aangeboden worden. UWV (KPN e.a.) is beheerder van de DNS van dit domein.
- Opdrachtnemer conformeert zich ten allen tijden aan de NCSC richtlijnen, en is verantwoordelijk voor het binnen redelijke termijn aanpassen van het https koppelvlak zodra NCSC haar richtlijnen wijzigt.

De te ontsluiten applicatie van inschrijver wordt via een proxy omgeving van UWV benadert. De proxy ondersteunt alleen prt 443, GEEN andere poorten.

**Hosting en housing**

Indien opdrachtnemer een on-premises oplossing biedt, dan is het mogelijk de applicaties van opdrachtnemer onder te brengen in een of meerdere datacenters van DXC Er zijn diverse mogelijkheden:

- Housing (rack, elektra, koeling, beveiliging, netwerkaansluiting)
- Hosting (virtual server, storage, Linux, Windows (N, N-1), Active/passive of Active/Active clusters, loadbalancing, backup en restore, patching, updates, Antivirus, LCM, rapportages, wijzigingsprocedures, remote Beheer etc.)
- De verantwoordelijkheden en procedures van / tussen DXC en Opdrachtnemer worden vastgelegd in een Operational Level Agreement (OLA).

**Koppelvlakken – Algemeen**

- Alle koppelingen met externe systemen / partijen worden getoetst door de UWV en KPN security officers
- UWV zal selectief pentesten uitvoeren op koppelingen van/naar externe partijen. Opdrachtnemer dient hier medewerking aan te verlenen
- Alle benodigde firewall policies t.b.v. aansluiten van de diensten van Opdrachtnemer op de UWV omgeving worden getoetst door de UWV en KPN security officers.

## 3. Algemene richtlijn voor technische levering/beschikbaarstelling van een ICT dienst.

De in een PvE uitgevraagde dienst dient beschikbaar gesteld te worden op de door KPN e.a. geleverde werkplek, netwerk, security en IAM infrastructuur van UWV. In het algemeen geldt dat KPN e.a. de connectiviteit realiseert tussen gebruikers / UWV infra en de ICT dienst. De UWV infrastructuur biedt 3 mogelijkheden voor Opdrachtnemer om de ICT dienst beschikbaar te stellen aan UWV:

- Vanuit het eigen datacenter van Opdrachtnemer, indien sprake is van een volledig door Opdrachtnemer te beheren private cloud dienst. KPN e.a. verzorgt in dat geval de aansluiting van het datacenter van Opdrachtnemer op het netwerk van UWV.
- Indien de aard van de dienst en het classificatieniveau van de te bewerken en verwerken gegevens dit toestaat en UWV hiermee akkoord is: Vanuit een door Opdrachtnemer beschikbaar gestelde SaaS omgeving op Internet.
- Vanuit het bedrijfsapplicatie-datacenter van UWV, beheert door DXC, op basis van housing of 3th party hosting. DXC levert de benodigde datacenter voorzieningen (incl DC LAN aansluiting) en koppeling naar het door KPN e.a. beheerde UWV gebruikersnetwerk.
    - I.g.v. housing levert en beheert Opdrachtnemer de applicatieservers en applicatie. Opdrachtnemer krijgt toegang via een beveiligde opstapomgeving.

Opdrachtnemer draagt zorg voor een actuele antivirus beveiliging en tijdige onderhoud/patching van de softwarestack.

- I.g.v hosting is Opdrachtnemer verantwoordelijk voor het Applicatiebeheer en stuurt Opdrachtnemer de leverancier DXC aan op het technisch Applicatiebeheer, inclusief het doorvoeren van releases en wijzigingen. Hosting is mogelijk op basis van Microsoft of Linux OS

Er is ook een mix denkbaar van bovenstaande mogelijkheden.