

Infrastructurele aansluitvoorwaarden voor ICT leveranciers van UWV

Auteur: J. Baas, IO&R

Versie: juni 2021

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 2022-2023 in beeld zodra betreffende diensten in die periode zijn 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 2022 tot en met eind 2023
- 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 2023 bereikt, uiterlijk 31-12-2023

2. 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.

3. Implementatie van de aansluiting van de ICT dienst

Opdrachtnemer stelt na gunning van de opdracht en voorafgaand aan de daadwerkelijke start van de dienstverlening een projectleider en een specialist ter beschikking. Zij geven beiden voorafgaand aan de start een toelichting op hun diensten aan KPN e.a., UWV en, indien van toepassing DXC, en geven hierbij aan op welke punten zij de samenwerking met KPN e.a. en/of DXC nodig achten.

Opdrachtnemer is verantwoordelijk voor de realisatie van de dienst, werkt hierbij nauw samen met KPN e.a en/of DXC en UWV, en fungeert hierbij als Service Integrator.

De opdrachtnemer zal - voor wat betreft imbedding in / aansluiting op de UWV infrastructuur - minimaal de volgende taken uitvoeren:

- Zorgen voor een projectmatige aanpak van ontwerp, bouw, test en oplevering van de integratie van de ICT dienst, en afstemming hiervan met derden en UWV
- Beschikbaar stellen van een projectleider, welke het aanspreekpunt voor de projectmanager van UWV en betrokken infra leveranciers (KPN e.a en/of DXC)
- Organiseren en leiden van de voortgangsvergaderingen met UWV en betrokken infra leveranciers
- Het opstellen van een Plan van Aanpak incl. planning en de wekelijkse voortgang rapporteren en toelichten
- Het inhoudelijk aansturen van de betrokken infra leveranciers (UWV zorgt vooraf voor de contractuele afspraken)
- Het coördineren van de door Opdrachtnemer zelf te verrichten werkzaamheden
- Het in samenwerking met de infra leveranciers en UWV opstellen van een high level design, zodat bij alle partijen helder is welke voorzieningen gerealiseerd moeten worden.
- Het schriftelijk doen van voorstellen voor beslissingen die door de opdrachtgever dienen te worden genomen. Dit betreft eveneens aangelegenheden die betrekking hebben op de aansturing van de betrokken infra leveranciers
- Het tijdig signaleren van knelpunten en risico's
- Aanspreekpunt zijn tijdens de uitvoering
- Organiseren van - en beschikbaar zijn tijdens de acceptatietest door UWV
- Oplevering van de benodigde beheer- en designdocumentatie.
- Het verlenen van medewerking bij de overdracht van de nieuwe dienst aan de beheerorganisatie van UWV en, voor zover van toepassing, aan de beheerorganisatie van de betrokken infra leveranciers.

Alle voor de implementatie noodzakelijke werkzaamheden en voorzieningen moeten zijn inbegrepen in de aanbieding.

4. Aansluitvoorwaarden gebruikersinterface

Beveiligde gebruikersinterface:

Voor het reguliere gebruik / bediening van de nieuwe dienst stelt de Opdrachtnemer een https interface beschikbaar. Via deze interface worden alle uit het PvE afleidbare eindgebruikers- en beheerfunctionaliteiten beschikbaar gesteld op een standaard UWV Werkplek met actuele browser. Voorwaarden gesteld aan de Werkplek incl. Browser staan in de specifieke infrastructurele aansluitvoorwaarden elders in dit document.

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

Authenticatie

Gebruikers van de door Opdrachtnemer te leveren ICT dienst worden geauthenticeerd en – indien van toepassing – geautoriseerd op basis van de Active Directory van UWV. Dit is een browserbased proces, op basis van Single Sign On, eventueel aangevuld met 2de factor authenticatie. De geldende voorwaarden ten aanzien van deze dienst worden in de specifieke infrastructurele aansluitvoorwaarden nader beschreven.

5. 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 VLANs, voor werkplekken (zgn. trusted LAN) en diverse doelgroepnetwerken van overige (ICT, facilitaire- en beveiligings) devices.
- Tevens is in alle lokaties Wireless LAN (WLAN) aanwezig. Het WLAN is gesegmenteerd naar doelgroepen: Besloten trusted / govroom voor internet toegang voor overheids-medewerkers / openbaar hotspot voor gasten.
- Het LAN en trusted WLAN van UWV gebruiken 802.1x toegangsbeveiliging. Devices dienen zich te authenticeren met een certificaat. Indien dit niet mogelijk is, geldt een geregistreerd MAC adres als authenticatiemiddel. Ongeauthenticeerde devices en BYOD's hebben geen toegang tot het LAN en trusted WLAN.
- Op het LAN is QoS ingericht. VOIP en video vallen onder de realtime klasse "platinum".
- Het LAN ondersteunt PoE

- 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 en proxy servers), alwaar Internet, datacenters en partner netwerken gekoppeld zijn.

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

- WLAN govroom is het primaire wifi netwerk voor UWV gebruikers. Authenticatie op basis van 802.1x certificaat of UID/PW, conform richtlijnen govroom. 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 MPLS verbindingen gebruikt worden
- Het WAN ondersteunt toegang tot internet, tot clouddiensten en tot datacenters van aangesloten leveranciers.
- Indien een locatie van Opdrachtnemer wordt aangesloten (hoofdzakelijk via internet), 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.
- Levering van een aansluiting van een nieuwe locatie kent een kortere doorlooptijd dan de CMO situatie
- Het WAN maakt gebruik van software defined centrale beveiligings-, routerings- en prioriteringsmechanismes. In overleg met Opdrachtnemer worden de beveiligingsparameters 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 lokaties 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 3^{de} 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.

Koppelvlak firewall UWV Koppeldienst (UKD) – FMO

- De UWV koppeldienst in de FMO situatie biedt dezelfde functionaliteit als de CMO
- de security diensten zullen zoveel omgebouwd zijn naar een Secure Web gateway / SASE / CASB set van functies, voor ICT diensten die als SAAS of cloud dienst worden aangeboden.
- Daarnaast zal een afgeschaalde 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 LDAP koppeling te realiseren, om users en rechtengroepen uit te lezen.
- Op de AD van UWV is het mogelijk een ADFS koppeling te realiseren, tbv federatieve authenticatie en autorisatie,
- Ondersteunde authenticatieprotocollen zijn: Kerberos, SAML, Openid-Connect, WS-FED. Een autorisatiemodule van een applicatie kan ook LDAP 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 FMO – belangrijkste verschillen met CMO

- LDAP(S) wordt niet meer ondersteunt
- 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 met alle ontwikkelingen geboden vanuit de Azure Active Directory functionaliteit.

Koppelingen

Koppelvlak internet / externe koppelingen:

- Externe koppelingen zijn mogelijk op de manieren IP-VPN, eigen WAN koppelvlak of via publiek internet (zonder beheerde koppeling)
- IP-VPN en WAN koppelvlakken zijn standaard aangesloten op de externe firewall
- Over de externe koppeling kan zowel de dienst als het beheer plaats vinden.
- Additioneel voorziet KPN in een Dienst Externe Toegang om - op naam gestelde - beheer werkzaamheden uit te voeren. Deze dienst is ontsloten via internet en voorzien van de noodzakelijke beveiliging (2-factor obv SMS) voor authenticatie en de verbinding.
- Uitgaande HTTP(S) koppelingen naar internet worden via de proxy dienst (zie elders in dit document) afgehandeld
- Inkomende HTTP(S) koppelingen vanaf Internet worden via de reverse proxy, of het Extern Koppelvlak van het UWV Systeemintegratie Platform afgehandeld. Dit vereist een ontwerp in overleg met UWV.

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 browsedienst

- Een intern bij UWV gehoste applicatie die incidenteel of structureel HTTP koppelingen nodig heeft naar Internet, dient dit via de proxy dienst van UWV te doen.
- De applicatie wordt op de proxy dienst geauthenticeerd op basis van zijn IP adres.
- De browsedienst voorziet in whitelisting van websites
- Een SaaS applicatie op internet wordt altijd via een proxy server/browsedienst benadert.

Koppelvlak mailrelay

- Indien een applicatie automatisch gegenereerde email verstuurd naar interne of externe ontvangers, dan moet deze email uit naam van uwv (uwv.nl) verstuurd te worden
- De applicatie dient de UWV mailrelay als next SMTP hop te gebruiken
- De applicatie wordt op de mailrelay geauthenticeerd op basis van zijn IP adres
- Indien opdrachtnemer gebruik maakt van eigen mailrelays of mailrelays van derden, en email uit naam van @uwv.nl verstuurd, dan moet het gebruikte SMTP en DNS koppelvlak voldoen aan de door de overheid verplichte standaarden voor veilige email: <https://www.forumstandaardisatie.nl>.

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

- Cloud based (SAAS) applicatie ontsluiting gebruikt altijd IE11 / Chrome / Edge Chromium, zonder plugins, op basis van HTML 5. De applicatie gebruikt de standaard proxy instelling.
- On prem applicatie ontsluiting:
 - bij voorkeur op basis van IE11/ Chrome / Edge Chromium, zonder plugins, op basis van HTML 5
 - Indien de zero footprint niet mogelijk is, biedt UWV de mogelijkheid plugins met App-V gevirtualiseerd aan te bieden.
 - Indien webbased applicatieontsluiting niet mogelijk is, biedt UWV bij uitzondering de mogelijkheid een applicatie-client met App-V gevirtualiseerd aan te bieden.
- Drivers voor randapparatuur zijn bij voorkeur Windows 10 logo gecertificeerd, en dienen aanvullend voor de UWV werkplek gecertificeerd te worden ivm de beveiligings-maatregelen 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.

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, electra, koeling, beveiliging, netwerkaansluiting)
- Hosting (virtuele 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)

Opdrachtnemer is verantwoordelijk voor middleware en applicaties.

- De keuze en inrichting is afhankelijk van de contractuele basis en de aard van de werkzaamheden en vereiste diensten, en daarom als maatwerk te ontwerpen, in samenspraak met UWV en DXC
- Opdrachtnemer dient gemaakte ontwerpkeuzes (en daaraan gerelateerde kosten) te onderbouwen, onder meer door deze te relateren aan de vereiste servicelevels omtrent beschikbaarheid en continuïteit.
- De verantwoordelijkheden en procedures van / tussen DXC en Opdrachtnemer worden vastgelegd in een Operational Level Agreement (OLA).

Apparatuur op vestigingen UWV

Hiervoor biedt UWV de dienst DOTR (Dienst omgeving technische ruimte) in de ICT-ruimtes MER's & SER's.

- De apparatuur op de vestiging van UWV dient door Leveranciers in een goede geconditioneerde en beveiligde ruimte geplaatst te worden. Hier zijn technische

ruimtes (MER & SER's) voor ingericht. D.m.v. de dienst "DOTR" (dienst omgeving technische ruimte) worden deze ruimtes bewaakt en beheerd.

- De dienst "DOTR" is een onderdeel van netwerkdienst wat uitgevoerd wordt door onze mantelleverancier KPN, zij functioneren als SPOC (single point of contact) en zijn verantwoordelijk voor de administratie, het beheer, onderhoud en de storingsafhandeling.

De toegang tot de BKN-kasten, High Availability Cabinets en vergelijkbare apparatuurskasten in de MER/SER-ruimtes verloopt via KPN voor de UWV panden. Waar UWV zit bij derden zijn afwijkende afspraken. Deze zijn op te vragen via RIC-ers (Regionale ICT Coördinatoren).

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 tbv aansluiten van de diensten van Opdrachtnemer op de UWV omgeving worden getoetst door de UWV en KPN security officers.