Infrastructurele aansluitvoorwaarden voor ICT leveranciers van UWV

Versie: aug 2021

1. 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 recente versies Microsoft of Linux OS

Er is ook een mix denkbaar van bovenstaande mogelijkheden.

2. Aansluitvoorwaarden gebruikersinterface

Beveiligde gebruikersinterface:

Voor het reguliere gebruik / bediening van de nieuwe dienst stelt de Opdrachtnemer (bij voorkeur) 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 on-prem bij DXC gehoste applicaties is het toegestaan dat, in geval de functionaliteit dit vereist, een client software package wordt ingezet, maar alleen in die gevallen dat dit niet anders kan. Voor SAAS applicaties is dit niet toegestaan

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 op basis van (federatieve) 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.

3. WAN

Koppelvlak WAN:

- 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%)
- Bandbreedte nader te bepalen, afh van de toepassing
- De WAN aansluiting van een datacenter heeft geen directe koppeling met het internet of andere externe netwerken of ICT diensten (geen backdoors). Al het verkeer loopt via het WAN en de centrale koppeldienst van UWV (UKD) met gestapelde securityfuncties (w.o. firewalls), alwaar Internet, datacenters van andere ICT leveranciers en partner netwerken gekoppeld zijn.

4. 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 DXC housing/colocation of DXC hosting diensten worden aangeboden aan UWV, dan is het koppelvlak met UWV standaard beschikbaar. Het DXC datacenter is reeds gekoppeld aan het UWV netwerk,

dus ontsluiting van de applicatie richting UWV gebruikers is na realisatie van de hosting/housing als vanzelf geregeld. Er zal voorafgaand aan de realisatie door DXC een ontwerp gemaakt worden, in samenspraak met Opdrachtnemer en KPN.
- Indien de ICT dienst van opdrachtnemer vanuit een SAAS omgeving op internet wordt aangeboden, dan 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.

5. Active Directory

Koppelvlak Active Directory:

- Alle gebruikers accounts, werkplekken van UWV maken deel uit van het Active Directory domein van UWV
- Rollen worden geregistreerd in het Autorisatie Beheer Systeem (ABS), door UWV beheerd. Deze rollen worden automatisch geprovisioned naar de Active Directory autorisatiegroepen
- Bij DXC gehoste Windows applicaties kunnen gebruik maken van de aanwezige trust relatie
- Op de AD van UWV is het tevens 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, tbv 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

6. 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 browsedienst

- Een intern bij UWV/DXC gehoste applicatie die incidenteel of structureel HTTPS 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

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

7. Werkplek

Koppelvlak werkplek:

- 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 een virtuele desktop en kan binnen en buiten UWV benaderd worden. Tevens dient de applicatie in voorkomende gevallen op een Windows 10 client (Laptop) te functioneren.
- Cloud based (SAAS) applicatie ontsluiting gebruikt altijd Edge Chromium, zonder plugins, op basis van HTML 5. De applicatie gebruikt de standaard proxy instelling.
- Voor ontsluiting van On Prem gehoste applicaties geldt :
    - bij voorkeur op basis van 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 via de applicatie provisioning mogelijkheden op de UWV werkplek
- Drivers voor randapparatuur (indien van toepassing) 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.

8. Hosting en housing

Indien opdrachtnemer een on-premises oplossing biedt, dan is het mogelijk de applicatie(s) 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 de in samenspraak met DXC 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).

9. 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/of KPN en//of DXC security officers.