Basisset (alleen de relevante onderdelen)
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. 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.

3. Aansluitvoorwaarden netwerk UWV

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.

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.

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.

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.

Aansluiteisen SI:

UWV is serviceprovider en biedt de API's aan waar Inschrijver aan moet voldoen.
Voor de gateway moet rekening gehouden worden met de volgende requirements:

SIP-AMG	Request-response	async, sync	https, SOAP, REST, Streaming(MTOM(/XOP) Streaming Compression) Certificaten API keys IAM*	xml, json	HTTP Basic Authentication TLS 1.2 op transportlaag (two-way) WS Security (optioneel): Signing (optioneel) Encryptie payload (optioneel), certifcaten