UWV Aansluitvoorwaarden infrastructuur ICT diensten SaaS

Inhoud

1 Aansluitvoorwaarden

Hieronder een opsomming van de aansluitvoorwaarden zoals UWV die hanteert. Deze voorwaarden zijn afgeleid van de meest recente variant van het interne UWV document "UWV Aansluitvoorwaarden infrastructuur ICT diensten".

1.1 Gebruikersinterface

Voor het reguliere gebruik / bediening van de SAAS dienst stelt de leverancier een https interface beschikbaar. Via deze interface worden alle eindgebruikers- en beheerfunctionaliteiten beschikbaar gesteld op een standaard UWV Werkplek met actuele browser.

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.

1.2 Internet koppelvlak UWV

De SAAS dienst dient gebruik te kunnen maken van het internet koppelvlak van de UWV werkplek omgeving.

- Standaard koppelvlak is HTTPS, prt 443.
- De UWV gebruikers benaderen de SAAS oplossing via een forward proxy (KPN).
- Binnen de UWV firewall en proxy omgeving wordt QOS niet ondersteunt.
- Het dataverkeer wordt door de proxy geïnspecteerd op malware en virussen.

1.3 Active Directory

De applicatie maakt geen gebruik van LDAP(S). Deze wordt niet meer ondersteunt door UWV. De standaard authenticatie voorziening voor de applicatie is AD FS, UWV biedt daarvoor een IDP, deze is via internet bereikbaar. UWV streeft altijd naar Single Sign On zodat een gebruiker automatisch wordt ingelogd op de bedrijfsapplicatie van de leverancier, mits de gebruiker de juiste autorisaties heeft voor deze applicatie

De leverancier zorgt voor de juiste Service Provider inrichting. Standaard protocollen zijn SAML 2.0 , OpenID-Connect, WS-FED. Hierbij dient er rekening mee te gehouden te worden dat de Active Directory dienst van UWV meegroeit met alle ontwikkelingen geboden vanuit de Azure Active Directory functionaliteit.

Alle gebruikers accounts en autorisaties 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.

De leverancier van de SaaS dienst dient aan te geven welke claims benodigd zijn voor het authenticatie en autorisatieproces.