

Annex XI-C - Beschrijving ICT-Karakteristieken:

Dit is een aanvullende beschrijving van het ICT- landschap zoals dat momenteel binnen HZ aanwezig is. Deze annex heeft uitsluitend een informatief karakter.

Waar het in deze beschrijving over informatiesysteem/informatiesystemen/oplossing(en) wordt gesproken, wordt ook het geautomatiseerd systeem bedoeld. Waar wordt gesproken over leverancier of aanbieder wordt in het kader van de 'Europese aanbesteding Geautomatiseerd informatiesysteem HRM/Salarisverwerking & aanverwante diensten 'de Inschrijver' bedoeld.

A. ALGEMENE KENMERKEN ICT-INFRASTRUCTUUR

De ICT-infrastructuur van HZ is de basis voor alle digitale ondersteuning, waaronder beschikbaarheid en gebruik van applicaties, de informatievoorziening en overige IT-voorzieningen. Het landschap wordt gekenmerkt door een variëteit aan applicaties, zowel standaard applicaties als maatwerk (zelfbouw). De IT-infrastructuur is gebaseerd op Microsoft Technologie; waaronder Microsoft Server, MS SQL databases, SQL Server Reporting Services en MS Office 365 Cloud. HZ gaat ervanuit dat Inschrijver een oplossing aanbiedt die past en functioneert binnen de hier beschreven ICT-Karakteristieken van HZ.

De ICT-infrastructuur van HZ is de basis voor alle digitale ondersteuning, waaronder beschikbaarheid en gebruik van applicaties, de informatievoorziening en overige IT-voorzieningen. Het landschap wordt gekenmerkt door een variëteit aan applicaties, zowel standaard applicaties als maatwerk (zelfbouw). De IT-infrastructuur is gebaseerd op Microsoft Technologie; waaronder Microsoft Server, MS SQL databases, SQL Server Reporting Services en MS Office 365 Cloud.

Toegang tot infrastructuur en systemen

Toegang tot informatiesystemen is anytime en anyplace mogelijk, maar altijd via de infrastructuur van HZ, namelijk via ADFS/SaML (FS.myHZ.NL). Gebruikers die rechtstreeks op een informatiesysteem proberen in te loggen worden door het informatiesysteem gerouteerd naar FS.myHZ.NL. Vanuit hier geldt het principe van single sign on. Op FS.myHZ.NL wordt gecheckt of de gebruiker al is ingelogd. Als dit het geval is wordt de applicatie opgestart. Indien de gebruiker nog niet is ingelogd, dan moet deze inloggen op FS.myHZ.NL, waarna de applicatie wordt opgestart. Deze procedure voor toegang tot de HZ ICT-infrastructuur en informatiesystemen geldt voor elke willekeurige locatie van waaruit gewerkt wordt, of dit nu binnen de gebouwen van HZ plaatsvindt of daarbuiten.

HZ streeft naar een eenduidige toegang tot interne- en externe webapplicaties, veelal aangeboden via het centrale medewerkersportaal via single sign-on. Hierbij wordt gestandaardiseerd naar een gefedereerde inlogmethode op basis van SAML2. Hierbij geldt SURFconext als inlogmethode voor Cloud/SaaS applicaties. Ten aanzien van toegang informatiesystemen geldt:

- a. (SSO) toegang tot self-service diensten / portal functies met het instellingsaccount op basis van een federatieve inlogprocedure (via SURFconext / SAML2)
- b. Mogelijkheid tot selectieve toepassing van 2 factor authenticatie bij het geven van toegang tot specifieke administratieve functionaliteiten (via SURFconext)
- c. Mogelijkheid tot selectieve afscherming van functionaliteiten via additionele netwerkbeveiliging (VPN tunnel via IPsec)
- d. Zolang er internetverbinding is moeten gebruikers ongeacht tijd, plaats en device, toegang kunnen krijgen de informatiesystemen.

SURFconext

Van leveranciers wordt verwacht dat zij aangesloten zijn of zich aanmelden bij SURFconext als serviceprovider (voor meer informatie en aanmelden van de service: [Get Conexted - SURFconext - Get Conexted - SURF Wiki \(surfnet.nl\)](#)). Hiermee wordt de hiervoor beschreven procedure voor toegang en sso, automatisch geregeld.

Multi Factor Authenticatie en SSO

HZ synchroniseert haar Active Directory naar Microsoft Azure Active Directory. Zoveel mogelijk dient authenticatie op basis van Single Sign On plaats te vinden, echter wel op de plek waar de daadwerkelijke authenticatie plaatsvindt. Voor HZ is dat FS.myHZ.NL. Dit betekent onder meer dat als een gebruiker al is ingelogd (bv op de MyHZ-portal) deze bij het opstarten van andere applicaties/informatiesystemen, niet opnieuw hoeft in te loggen.

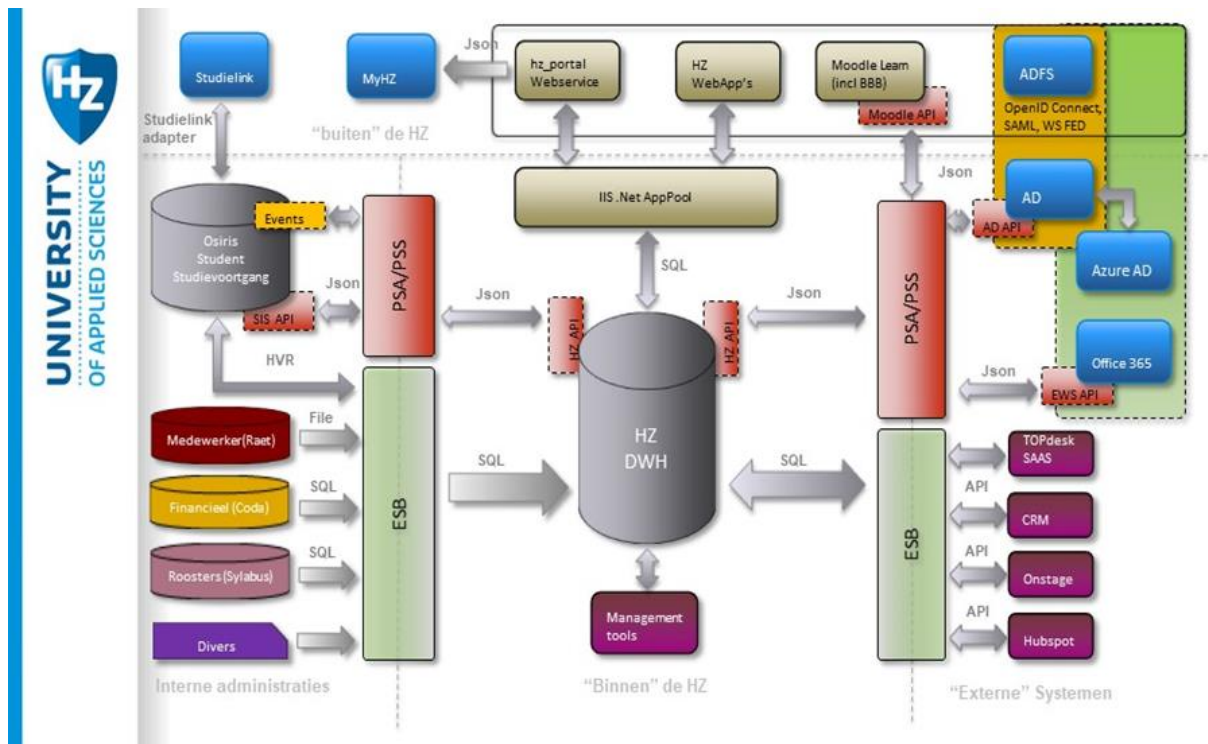
HZ maakt gebruik van MFA vanuit Azure en koppelt deze met SURFconext (zie: [SURFconext: overal veilige toegang met 1 set credentials | SURF.nl](#)). Toegang tot de HZ ICT-infrastructuur en informatiesystemen vindt altijd plaats op basis van MFA (tenminste 2FA), dit maakt onderdeel uit van de hierboven beschreven toegangsprocedure en SURFconext procedure.

Microsoft-licenties

Indien voor (onderdelen van) informatiesystemen of oplossingen specifieke Microsoft licenties vereist zijn, dan geldt dat deze licenties zullen worden betrokken via SURF, voor zover deze nog niet zijn aangeschaft door of in het bezit zijn van HZ.

B. AANSLUITING OP TECHNISCHE OMGEVING C.Q. SYSTEEMCONTEXT – HZ-KOPPELVLAKE

Onderstaande figuur is een vereenvoudigde weergave van het applicatielandschap en de onderlinge applicatie-interacties van HZ. Informatiesystemen krijgen hierin hun plek, waarbij voor uitwisseling met andere systemen/oplossingen, sprake zal zijn van ontvangst en levering van gegevens van en aan het HZ-Koppelvlak via API's. Met het HZ-Koppelvlak wordt hier de afgebeelde PSA/PSS en ESB bedoeld.



PSA: Process State API - Endpoint waar data opgehaald en verwerkt kan worden;

PSS: Process State Server – Windows Service.

Deze weergave laat zien dat systemen niet rechtstreeks met elkaar zijn verbonden. Zo lopen er geen directe lijntjes van b.v. het HRM (Raet) systeem naar e.g. Osiris, OnStage, Active Directory of Syllabus. De PSA (i.c.m. ESB (Enterprise Service Broker), welke we uit willen faseren voor de PSA) zorgt ervoor dat de output van bronsystemen als input gebruikt wordt voor ontvangende systemen.

HZ werkt met PSA/PSS en (nu nog) een Enterprise Service Bus (ESB)¹ in combinatie met een Data warehouse voor het uitwisselen van gegevens tussen de diverse informatiesystemen (het HZ-Koppelvlak). Informatiesystemen die als leidend bronsysteem voor specifieke informatiegroepen zijn aangewezen, moeten op basis van specifieke, individuele events (real-time) informatie aanbieden aan het HZ-Koppelvlak. HZ hanteert het principe dat gegevens eenmalig binnen de volledige infrastructuur van HZ ingegeven moeten worden (geen dubbele invoer). Informatiesystemen die niet leidend zijn, maar wel over bepaalde gegevens moeten beschikken, moeten (real-time) gegevens kunnen ontvangen uit het HZ-Koppelvlak. De gegevensuitwisseling (aanleveren en ontvangen) moet plaatsvinden op het moment dat de individuele events plaatsvinden, tenzij specifiek door HZ wordt aangegeven dat batch-uitwisseling van toepassing is. Berichtenverkeer/gegevensuitwisseling wordt op basis van in overleg af te stemmen triggers geïnitieerd voor verzending en ontvangst.

Het HZ-koppelvlak is niet rigide, geen vastomlijnde voorschriften over welke gegevens in welk format moeten worden aangeleverd. HZ draagt zelf zorg voor ontwerp en realisatie van het HZ-Koppelvlak. Leverancier dient ervoor te zorgen dat het aangeboden informatiesysteem in staat is om gegevens te sturen naar en te ontvangen van het HZ-Koppelvlak.

Relevant voor informatiesystemen is:

- a. Beschikbaarheid van een gedocumenteerde Application Programming Interface (API) om gegevens uit te kunnen wisselen tussen het specifieke (geleverde) informatiesysteem en andere applicaties (via het HZ-Koppelvlak).
- b. Webservices/ interfaces/protocollen voor gestandaardiseerde communicatie tussen informatiesystemen zijn gebaseerd op SOAP, REST, HTML, WebApi en/of JSON.
- c. Standaard Exportmogelijkheden/ uitvoermogelijkheden naar XML, PDF, CSV, Excel.

Voor gegevens waarvan andere informatiesystemen de bron vormen (dus leidend zijn), wordt afgesproken welke gegevens wel en niet in het ontvangende systeem mogen worden aangepast. Voor deze gegevens zal altijd gelden dat ontvangen brongegevens de waarde in het ontvangende systeem zullen overschrijven (ook als deze dus al eerder in het ontvangene systeem waren aangepast en daarmee afwijken van de bron).

C. INFRASTRUCTUUR KENMERKEN

De infrastructurele kenmerken en eisen van HZ worden onderverdeeld naar:

- WAN- infrastructuur
De WAN infrastructuur betreft de verbinding van/tussen alle fysieke locaties van HZ. Dit zijn: 1X HZ-Gebouwen en terrein Vlissingen (inclusief de HZ-Toren), 1x HZ-gebouw en terrein Middelburg. Daarnaast is nog sprake van de samenwerkingslocatie Roosendaal. Deze wordt echter als een externe locatie gezien; verbinding met de WAN-infrastructuur vindt plaats via HZ-VPN. Binnen de infrastructuur van HZ (Vlissingen en Middelburg) is alles ondergebracht in 1 domein.
- Back-end infrastructuur
Dit betreft de infrastructuur voor alle (interne en externe) medewerkers van HZ, denk aan de apparatuur en systemen die (nog) on-premises staan.

Backups en Uitwijk: In geval van SaaS-oplossingen dienen leveranciers zorg te dragen voor het borgen en verzorgen van Uitwijk en van backup & restore activiteiten, inclusief de data (indien van toepassing, met uitzondering van overeengekomen opslag binnen de eigen infrastructuur van HZ).

Van desktops en laptops wordt geen backup gemaakt. Dit is de verantwoordelijkheid van de gebruiker zelf. Gebruikers wordt (dringend) geadviseerd bestanden en data zoveel mogelijk centraal op te slaan (servers, Teams/Sharepoint). Buiten Teams is er geen specifiek DMS beschikbaar; Teams wordt niet als formeel DMS gebruikt.

- LAN- infrastructuur
De infrastructuur waarmee de werkplekken/devices van de medewerkers worden gekoppeld aan de back-end infrastructuur. Er is sprake van bekabelde (desktops en dockingstations) en draadloze (Wifi) verbindingen (laptops en andere devices).

SaaS en Connectiviteit

HZ neemt in toenemende mate en bij voorkeur applicaties volgens het SaaS (Software-as-a-Service) af. Hierbij wordt de organisatie wat betreft technisch beheer ontzorgd en kan de nadruk op de 'business' zelf komen te liggen. Bij de keuze voor SaaS-oplossingen geldt dat de gebruikerskant browser-/web-based en de serverkant cloud-based (vanuit HZ gezien) moet zijn. Alle connectiviteit van en naar SaaS-applicaties dient naast IPv4 ook IPv6 te ondersteunen;

Beschikbaarheid, eigendom en portabiliteit van data:

HZ blijft te allen tijde eigenaar van de data (masterdata en transactiegegevens) in informatiesystemen en gerelateerde oplossingen, onafhankelijk of deze binnen of buiten de infrastructuur van HZ worden opgeslagen.

Portabiliteit van gegevens: Leveranciers van informatiesystemen en gerelateerde oplossingen voorzien in een data-migratiestrategie zodat HZ in staat gesteld wordt de actuele gegevens te migreren naar een ander platform (bijvoorbeeld ter voorkoming van vendor lock-in).

Security en Informatiebeveiliging

HZ hanteert de NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS). Zie ook: <https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1>

SURF- normenkader

Vanuit het SURF normenkader is een overzicht van security requirements opgesteld welke standaard onderdeel zijn van de ICT-vereisten van HZ die aan leveranciers van informatiesystemen en gerelateerde diensten en oplossingen worden gesteld. Het betreft de Baseline informatiebeveiliging ([baseline-informatiebeveiliging-ho-2015.pdf \(surf.nl\)](#)).

Toegankelijkheid systeem

HZ zet in op het platform- en plaats-onafhankelijk aanbieden van haar dienstverlening. Hierbij legt HZ de nadruk op functionaliteit en gegevensbronnen die via het netwerk (Cloud) worden aangeboden. Hierbij is platformonafhankelijk van groot belang. Dit wordt bereikt door de toepassing van open standaarden en het realiseren van optimale toegankelijkheid voor verschillende 'devices'. Wat betreft de 'user' interfaces zijn de kenmerken:

- a. Web interfaces op basis van HTML5 standaarden (geen gebruik van plugins/ helpers e.d) en web-interfaces worden ondersteund door alle gangbare webbrowsers die HTML5 ondersteunen.
- b. Gebruikersinterfaces zijn geschikt voor Windows en ingeval van mobile devices voor Android en iOS.
- c. Web interfaces zijn geschikt voor zowel werkstations als mobiele devices (responsive interfaces)
- d. Indien leveranciers apps beschikbaar stellen, ondersteunen deze zowel de ios (Apple) als Android (Google) platformen.

Gegevensbescherming en beveiliging

HZ is een professionele, verantwoordelijke en publiek gefinancierde instelling. Als zodanig neemt zij gegevensbeveiliging en -bescherming, privacy en vertrouwelijk uiterst serieus. Voor het

informatiesystemen die als SaaS / -Cloud-based / Web-based oplossing worden aangeboden/afgenomen, wordt deze verantwoordelijkheid noodzakelijkerwijs gedeeld tussen HZ en Inschrijver.

Leveranciers van informatiesystemen voldoen aan hoge informatiebeveiligingseisen (ISAE3402, ISO27001 of gelijkwaardig) en hebben hun beheersmaatregelen geoptimaliseerd, ter voorkoming van inbreuk, falen, lekken en onrechtmatige verwerking. Een externe auditor kan hierop controleren.

Als zodanig stelt HZ de volgende eisen aan aanbieders van informatiesystemen:

- a. Verwerkt een andere organisatie namens de HZ persoonsgegevens? Dan is de HZ volgens de Algemene verordening gegevensbescherming (AVG) verplicht om een overeenkomst op te stellen met de verwerker (leverancier). Dit wordt gedaan middels een verwerkersovereenkomst. In deze verwerkersovereenkomst moet nadrukkelijk worden omschreven wat de exacte afspraken zijn tussen de verwerkingsverantwoordelijke (de HZ) en een verwerker (de leverancier). Zie <https://autoriteitpersoonsgegevens.nl> voor meer informatie. Deze overeenkomst regelt verantwoordelijkheden van HZ en Inschrijver met betrekking tot de bewerking van persoonsgegevens en de afhandeling van incidenten bij inbreuk. Voldoet aan vigerende wet- en regelgeving, bijvoorbeeld meldplicht datalekken.

Inschrijver hanteert de verwerkersovereenkomst van HZ. Eventuele 3^e partijen die Inschrijver inzet dienen hierin als subverwerker te worden vermeld.

- b. Inschrijver committeert zich bij vermoedelijke en optredende datalekken aan het direct informeren van de HZ, inclusief opgaven van de gegevens, de omvang hiervan, acties om de impact te reduceren en acties om dergelijke datalekken in de toekomst te voorkomen.
- c. Inschrijver draagt ervoor zorg dat er proactief oplossingen worden aangereikt en/of maatregelen worden getroffen ter voorkomen van beveiligingslekken (o.a. CVE's - [Common Vulnerabilities and Exposures - Wikipedia](#))
- d. Persoonsgegevens mogen alleen worden opgeslagen in landen die vallen onder het adequaatsheidsbesluit van de EU of waar een passend beschermingsniveau wordt gewaarborgd en vastgelegd in de EU standard contractual clauses (SCC's). Geen gegevens buiten EER.
- e. Opslag van de gegevens in de Verenigde Staten is niet toegestaan. Het US privacy shield is sinds juli 2020 *niet* langer geldig en ook het gebruik van SCC's is problematisch, aangezien verwerkingsverantwoordelijke verantwoordelijk is voor de controle en handhaving van voldoende waarborgen.
- f. Gezien de aard van de gegevens is een Privacy impact assessment verplicht. Inschrijver dient alle medewerking te verlenen bij het verrichten van Privacy Impact Assessment (welke maatregelen zijn getroffen) zoals opgenomen in bijlage II a met invulinstructie bijlage II b. MFA dient buiten HZ altijd aan te staan, gezien de vertrouwelijkheid en aard van de gegevens. Daarbij dient applicatie-beheerder altijd MFA te krijgen en daarbij kan alleen binnen HZ toegang worden gekregen (of eventueel via VPN).
- g. Leveranciers van informatiesystemen gaan akkoord met de standaard verwerkersovereenkomst van SURF (zie Annex IV-B).

OTAP

Voor aanbieders van Cloud, SaaS of Web-based informatiesystemen geldt dat er tenminste 2 applicatieomgevingen (acceptatie en productie) beschikbaar dienen te zijn:

1. Acceptatieomgeving
Nieuwe releases worden voor in productie name altijd eerst beschikbaar gesteld in de acceptatieomgeving en de ontwikkel/zandbak-omgeving. In de Acceptatie omgeving wordt de definitieve instelling en inrichting getest en getoetst. Na akkoord wordt via een vastgestelde procedure de inrichting overgezet naar de productieomgeving.
2. Productieomgeving
Dit is de daadwerkelijke omgeving waarin de productie wordt gedraaid en dus de reguliere, dagelijkse, wekelijkse, maandelijkse en jaarlijkse werkzaamheden/verwerkingen plaatsvinden.
3. Optioneel: Ontwikkelomgeving / Zandbak
HZ wil kunnen experimenteren en ook in relatie tot rapportages, dashboards en het HZ-Koppelvlak (mee) kunnen ontwikkelen aan gegevensuitwisseling. Dit vindt bij voorkeur plaats binnen een aparte ontwikkel- of zandbak-omgeving.

Leveranciers van informatiesystemen faciliteren dat op verzoek van HZ altijd een kopie van de inrichting en data van productieomgeving kan worden overgezet naar de ontwikkel-/zandbak-omgeving en de acceptatieomgeving.

Onderhoud en onderhoudswindow

HZ zal momenten en perioden per jaar kunnen aanwijzen waarop geen onderhoud kan worden gepleegd door leveranciers van informatiesystemen. Voor de onderhoudswindows geldt dat onderhoud niet per definitie buiten kantooruren hoeft plaats te vinden. Zeker waar onderhoudswerkzaamheden gepaard gaan met of opgevolgd moeten worden door acties/handelingen door/bij HZ, verdient het de voorkeur dit tijdens kantooruren, maar in ieder geval in overleg met HZ te plannen.