Bijlage A-004
Huidige en toekomstige situatie

Netwerkdiensten

Mededingingsprocedure met onderhandeling

Versie 1.0
2 februari 2022

1. Inhoudsopgave

2. Inleiding

UWV heeft op dit moment zijn Kantoorautomatisering, Werkplekdiensten, Netwerkdiensten, Telefonie, Contactcenter en aanverwante diensten (hierna KWNTC) uitbesteed aan diverse externe leveranciers. De contracten hiervoor met KPN, BT en Capgemini dienen opnieuw aanbesteed te worden. In 2020 is een vooronderzoek uitgevoerd met als doel de toekomstvisie en de (daarop gebaseerde) sourcing strategie voor de gehele KWNTC-scope te bepalen. In het vooronderzoek is onder andere gebruik gemaakt van een marktconsultatie met interactie en referentiegesprekken om zo een goed beeld te krijgen van marktontwikkelingen, kansen en risico's. Het vooronderzoek is eind 2020 afgerond en heeft geresulteerd in een vastgestelde toekomstvisie en sourcing strategie voor de gehele KWNTC-scope.

In de sourcing strategie zijn verschillende scenario's voor verkaveling onderzocht. De scenario's zijn daarbij gewogen en beoordeeld op sourcing doelstellingen. Op basis van de uitkomsten van het vooronderzoek is besloten dat de Netwerkdiensten als (apart) kavel worden aanbesteed.

De netwerkdiensten maken op dit moment onderdeel uit van de overeenkomst met KPN. Deze overeenkomst heeft betrekking op de Kantoorautomatisering-, Werkplek- en Netwerkdiensten (KWN) en eindigt op 31 december 2023.

Via deze aanbesteding wil UWV de Netwerkdiensten verwerven die aansluiten op de overige kavels (zie paragraaf 3.1 en 4.1) en het programma Samen naar de Moderne Werkplek (SMW).

2.1 *Leeswijzer*

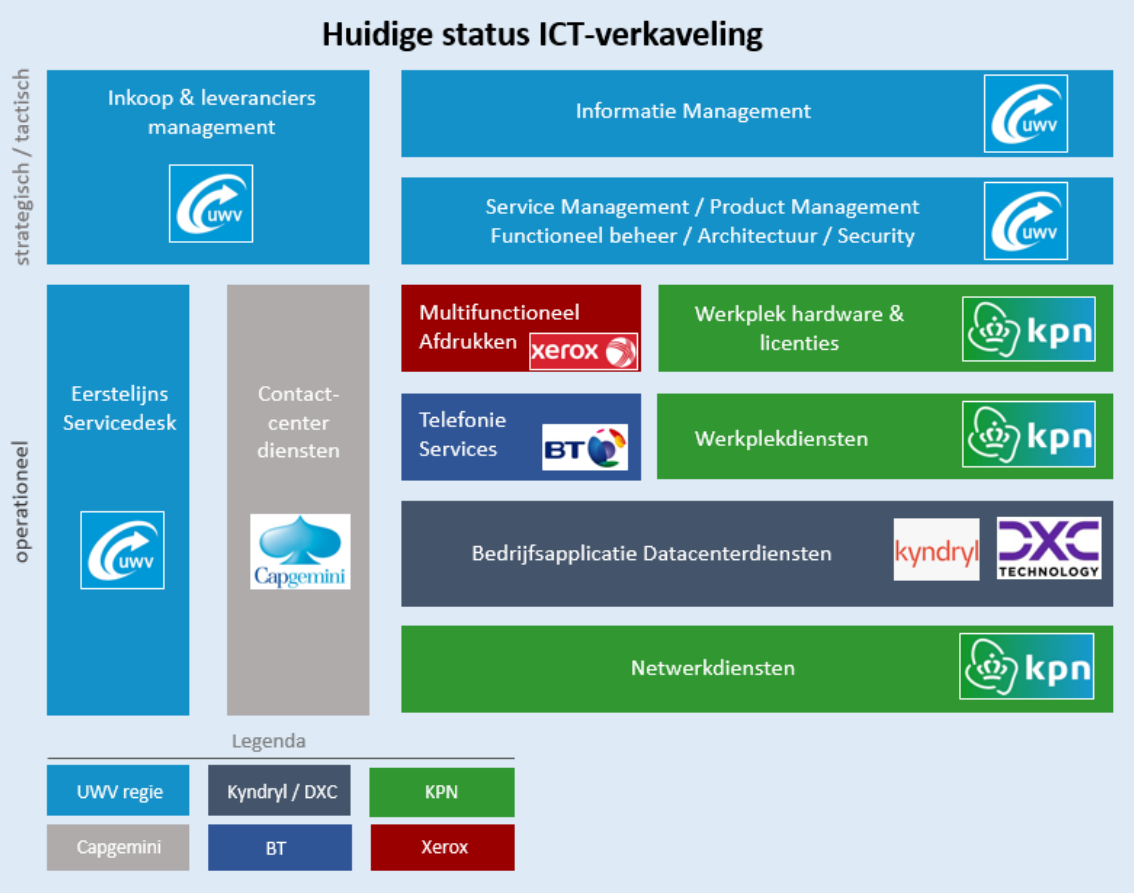
Deze 'Bijlage A-004 Huidige en toekomstige situatie' geeft de globale scope van de aanbesteding Netwerkdiensten weer. In de selectiefase van de aanbesteding verstrekt UWV geen details over de inrichting van de Netwerkdiensten. De gedetailleerde uitwerking wordt beschikbaar gesteld in de volgende fase: de gunningsfase.

De diensten in de huidige situatie worden in hoofdstuk 3 op hoofdlijnen beschreven. In hoofdstuk 4 worden de toekomstige diensten in scope van de aanbesteding beschreven.

3. Beschrijving van de huidige situatie

3.1 *Huidige ICT-verkaveling*

De huidige netwerkdiensten worden vanuit het huidige KWN-contract door KPN geleverd. Onderstaande Figuur 1 geeft op hoofdlijnen de huidige ICT-verkaveling van UWV weer. De groen gemarkeerde diensten betreffen de KWN-diensten die KPN aan UWV levert.



Figuur 1: Huidige status ICT-verkaveling

In Figuur 1 zijn verschillende ICT-kavels gedefinieerd op strategisch/tactisch- en operationeel niveau. De onderstaande Tabel 1 geeft een beknopte beschrijving van elk van deze kavels.

Strategisch- ,tactische-, en operationele regievoering:	
Inkoop & leveranciers management	Borgt optimale inkoop en levering van kwalitatieve diensten en producten die aansluiten bij de ICT behoefte van de business
Informatie management	Beheert en draagt zorg voor een optimale informatie uitwisseling door het aanbieden van een breed palet aan communicatiemiddelen
Service management	Draagt zorg voor een juiste naleving van de Service Level Agreement (SLA) en Dossier Afspraken en Procedures (DAP), welke overeengekomen zijn tussen UWV, leveranciers en partners

Product management	Draagt zorg voor de bewaking van de levenscyclus van ICT-diensten en producten. Hier valt onder de ontwikkeling, verwerving, beheer en de uitfasering van ICT-diensten
Functioneel beheer	Draagt zorg voor het optimaal laten functioneren van één of meerdere informatiesystemen
Architectuur	Sturende rol in het verkrijgen en uitdragen van inzichten in de samenhang van de bedrijfsstrategie, informatievoorziening en ICT
Security	Draagt zorg voor een juiste borging van het informatie-beveiligingsbeleid binnen de bestaande- en nieuwe ICT-diensten
Eerstelijns servicedesk	UWV servicedeskorganisatie waar service verzoeken en incidenten voor alle ICT-diensten en bedrijfsapplicaties worden gemeld
Kavels operationele diensten	
Contactcenter diensten	Uitbestede dienst: het leveren en afhandelen van telefoongesprekken, chat- en e-mail communicatie
Multifunctioneel afdrukken	Uitbestede dienst: print-, scan-, fax-, en kopieerdienst
Telefonie services	Uitbestede dienst: het leveren van vaste en mobiele telefonie, bijbehorende hardware, indoordekking en berichtendienst
Werkplek hardware & licenties	Uitbestede dienst: het leveren van werplekhardware en accessoires. En daarnaast het leveren van licenties
Werkplekdiensten	Uitbestede dienst: het leveren en beheren van de complete ICT werkplekoplossing en aanverwante diensten. Belangrijke onderdelen zijn de virtuele werkplekdiensten, Active Directory en Mobile Device Management (MDM)
Bedrijfsapplicatie Datacenterdiensten	Uitbestede dienst: het leveren van infrastructuur, hosting, technisch applicatiebeheer en cloud broker rol
Netwerkdiensten	Uitbestede dienst: het leveren van netwerk- en security infrastructuur en aanverwante diensten

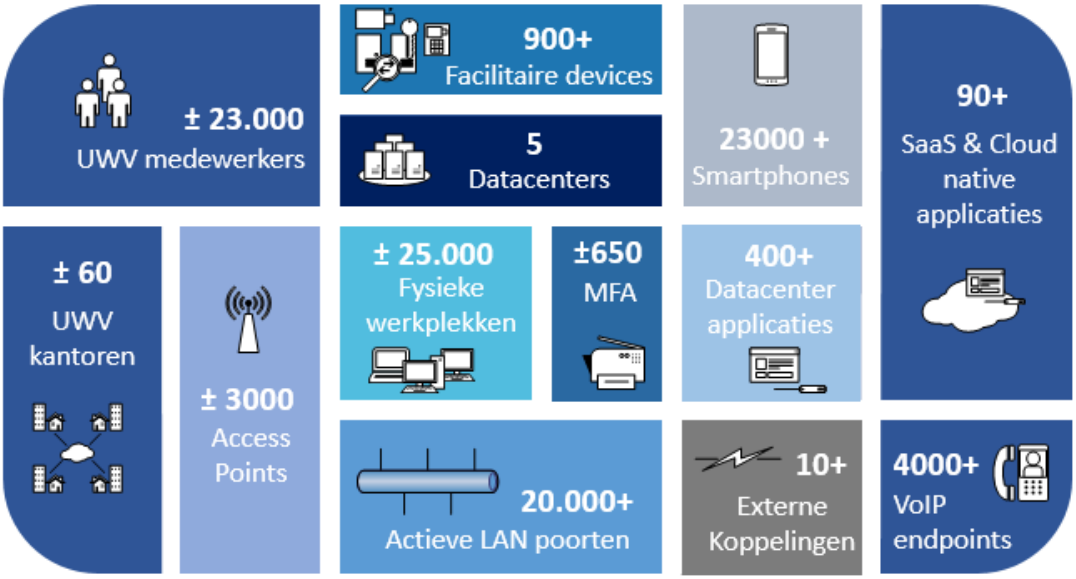
Tabel 1: korte beschrijving van ICT-kavels

3.2 *Inrichting huidige netwerkdiensten*

De netwerkdiensten zoals weergegeven in Figuur 1 omvatten:

- Netwerkdiensten op kantoren;
- Centrale netwerkdiensten;
- Centrale en decentrale netwerkbeveiligingsfuncties;
- Benodigde operationele en tactische beheerdiensten;
- Koppelvlakken naar overige kavels en externe (keten)partners.

De dienst is volledig uitbesteed en maakt integraal deel uit van de huidige KWN-kavel en het KWN-contract. Op een aantal aspecten, zeker op het vlak van beheerprocessen, zijn dienstonderdelen daarom geïntegreerd met de werkplekdiensten.
Onderstaande Figuur 2 geeft inzicht in de omvang van de huidige situatie. Alle beschreven kengetallen zijn indicatief.

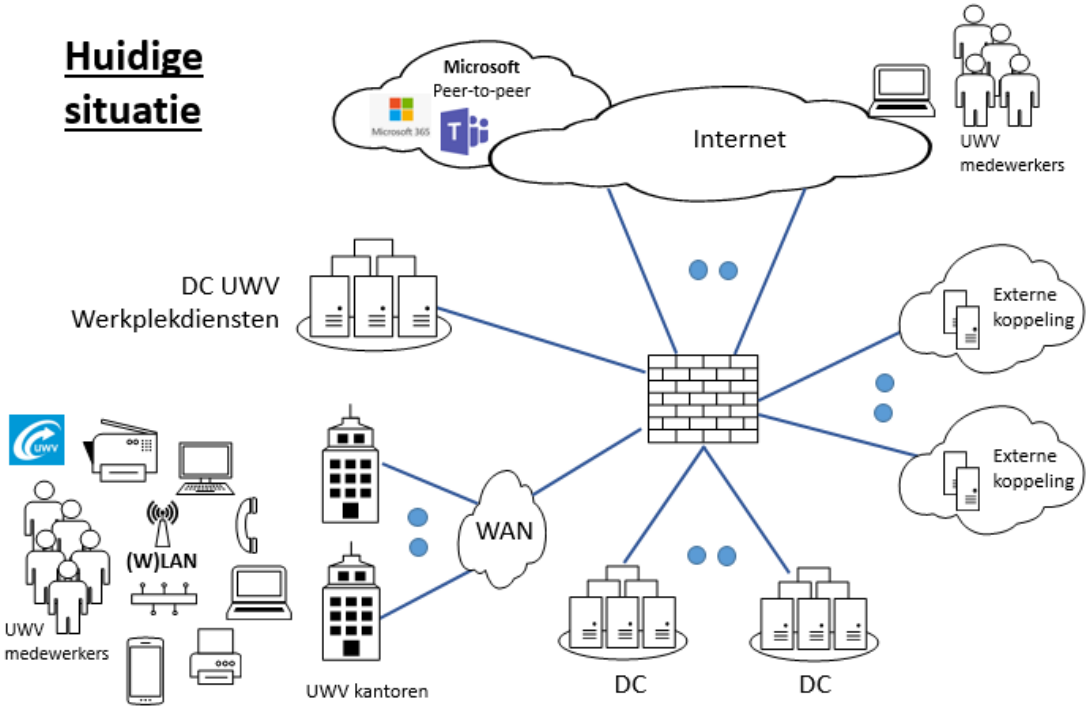


Figuur 2: Relevante aantallen netwerkdiensten

De huidige netwerkdiensten bieden een managed (Wireless)LAN en MPLS WAN voor circa 60 kantoren, ten behoeve van circa 23.000 gebruikers. Op het centrale koppelpunt bestaande uit onder andere firewalls zijn vijf (twin-)datacenters, diverse externe koppelingen met (keten)partners en een viertal centrale internetverbindingen aangesloten. De dienst wordt geleverd inclusief interne en externe DNS, SMTP relay, DHCP, IP adresbeheer en beheerdiensten voor het bedrijfskabelnetwerk (BKN) en MER's/SER's.

De netwerkbeveiligingsfuncties zijn gerealiseerd middels centraal gestapelde appliances voor inspectie, filtering en preventie. Tevens is er op en naar de kantoren VLAN segmentatie en Policy Based Networking geïmplementeerd. Aanvullend worden door de huidige netwerkleverancier de internetontsluiting van E-diensten (reverse proxy inclusief web application firewall (WAF), PKIoverheid, eHerkenning en Content Delivery Network (CDN) diensten) geleverd. In de huidige situatie maken deze diensten onderdeel uit van de scope van de netwerkdiensten.

Onderstaande Figuur 3 biedt een schematische weergave van de huidige situatie van het UWV-netwerk.



Figuur 3: Schematische weergave van de huidige situatie van het UWV-netwerk

De inrichting van de huidige netwerkdiensten is gedurende de aanbesteding onderhevig aan veranderingen. Deze veranderingen zijn het gevolg van de doorontwikkeling van bestaande ICT-kavels en diensten, zoals het programma SMW De beschrijving van de huidige situatie in de volgende hoofdstukken betreft dan ook de situatie ten tijde van de publicatie van deze bijlage A-004.

De netwerkdiensten zijn globaal onder te verdelen in de volgende vier hoofdcategorieën: netwerkdiensten (hoofdstuk 3.3.1), securitydiensten (hoofdstuk 3.4), beheerdiensten (hoofdstuk 3.5), en koppelvlakken (hoofdstuk 3.6). In de volgende hoofdstukken wordt dieper ingegaan op de inrichting per hoofdcategorie.

3.3 *Basis netwerkdiensten*

3.3.1 (Wireless) Local Area Network

Onze huidige leverancier (KPN) levert het draadloos en bedraad Local Area Network (LAN) op circa 60 kantoren van UWV. Deze kantoren bevinden zich in de grotere steden in Nederland. Het netwerk ondersteunt segmenten voor diverse doelgroepen zoals bijvoorbeeld UWV medewerkers en hun werkplek devices, bezoekers, printers en diverse facilitaire diensten. Het LAN is gebaseerd op een uniform en modulair ontwerp, en gaat uit van verschillende kantoormodellen. De omvang van een kantoor, en/of de aard van de activiteiten in een kantoor bepalen de mate van redundantie (alternatieve paden) van het LAN. En daarmee tevens de samenstelling van het aantal en type switches. Het LAN ondersteunt 100 Mbps en 1 Gbps poorten en biedt Power over Ethernet voor de WLAN Access points en VoIP devices.

Het draadloze LAN (Wireless LAN) van UWV vormt een geïntegreerd onderdeel van de LAN architectuur. Het Wireless LAN bestaat uit ruim 3000 access points en centraal opgestelde Wireless LAN Controllers (WLC's). Hierdoor wordt in alle kantoor- en algemene ruimtes (lobby's, bedrijfsrestaurants, vergaderruimtes, etc.), gegarandeerde dekking geboden. In de doorstroomruimtes zoals trappenhuizen, liften en verbindingsgangen is dekking niet

gegarandeerd. Op het Wireless LAN zijn een aantal SSID's beschikbaar. Elk voor een specifieke doelgroep (UWV intern, govroam, KPN HotSpot) en met de daarvoor benodigde technische- en functionele instellingen.

In het Wireless LAN en op alle LAN-poorten in de kantoren van UWV vindt authenticatie plaats door middel van de Policy Based Netwerk (PBN) dienst. De PBN dienst is gekoppeld met de Active Directory (AD) van UWV. De UWV AD behoort tot de werkplekdiensten.

3.3.2 Wide Area Network

Naast het wireless- en bedraad LAN levert de huidige leverancier het Wide Area Network (WAN) naar de kantoren van UWV. Het netwerk is gebaseerd op WAN MPLS technologie en is onderdeel van het KPN ONE netwerk.

Vrijwel alle kantoren van UWV zijn aangesloten via glasvezelverbindingen. De omvang van een kantoor en/of de activiteiten in een kantoor bepalen de mate van redundantie van de WAN-aansluiting. Tevens wordt hierdoor de toegekende bandbreedte bepaald. Bandbreedtes variëren tussen de 20 Mbps en 1 Gbps. Er kan in de meeste gevallen zonder vervanging van hardware of infrastructuur, bandbreedte worden bij- of afgeschakeld. De beschikbare bandbreedte wordt via een verdeelsleutel verdeeld over de diverse doelgroepen (zie paragraaf 3.3.2) die op het WAN ondersteund worden.

In het netwerk zijn Quality of Service (QoS)/Class of Service (CoS) profielen in gebruik. Dit zorgt voor een optimale bandbreedteverdeling en prioriteitstelling voor specifieke verkeersstromen zoals VoIP, videobellen, videostreaming en virtuele werkplekken. Aanpassingen op deze QoS/CoS-profielen zijn tevens een integraal onderdeel van de huidige dienstverlening van KPN. In het LAN, op devices en op relevante koppelingen wordt het verkeer voorzien van een markering die door de QoS/CoS-mechanismes in het WAN wordt herkend.

De benodigde bandbreedtes zijn afgestemd op de volumes van de diverse verkeersstromen. De belangrijkste verkeersstromen zijn:

- Verkeer tussen werkplekken op kantoor en de UWV virtuele werkplekdienst;
- VoIP verkeer tussen de soft- en hardphones op het LAN en vanuit/naar de Telefoniedienst en Contactcenter diensten;
- Applicatief verkeer tussen de virtuele werkplekken in het KPN-datacenter en de bedrijfsapplicatiedatacenters van Kyndryl en DXC;
- Teams videoverkeer (voornamelijk ten behoeve van videovergaderen) tussen de werkplekken op kantoor en de internet breakout richting Microsoft 365;
- Browse-verkeer tussen govroam en KPN HotSpot Wireless LANs en het internet.

Het verkeer tussen thuiswerkende medewerkers van UWV en de virtuele werkplek wordt afgehandeld door de internet breakout/opgang van de UWV-werkplekdienst (zie ook paragraaf 3.3.4).

3.3.3 Datacenter-aansluitingen en externe koppelingen

Vanuit de datacenters van de huidige netwerkdienstverlener KPN zijn via koppelvlakken (zie ook paragraaf 3.6) de externe partijen, netwerken en overige ICT-leveranciers aangesloten. Deze koppelvlakken zijn door middel van centrale beveiligingsfuncties (zie paragraaf 3.4.2) voorzien van de juiste beveiligingsmaatregelen.

Via (redundante) WAN-verbindingen zijn vijf (twin-)datacenters en diverse externe koppelingen met (keten)partners aan het netwerk van UWV gekoppeld. Het betreffen de volgende (twin-)datacenters:

- Business Applicaties en E-diensten van Kyndryl en DXC;
- (Virtuele) werkplek en kantoorautomatisering van KPN;
- Contactcenter diensten van Capgemini/Odigo.

Op de datacenter-verbindingen van Kyndryl en DXC geldt een scheiding van verkeersstromen op basis van VRF-techniek (Virtual Routing & Forwarding). Door deze VRF-techniek worden het interne applicatieverkeer en het internetverkeer naar websites van UWV van elkaar gescheiden. Alle dataverbindingen voldoen aan de beveiligingseisen zoals deze worden gesteld door het Nationaal Cyber Security Centrum (NCSC).

Binnen de (via het WAN ontsloten) KPN datacenters worden de volgende diensten gehost:

- De VoIP-centrales behorende bij de telefoniedienst van BT;
- Centrale omgeving van de Print/Kopieer/Fax/Scan dienst van Xerox.

Onderstaande datacenterdiensten van KPN zijn via beveiligde Data Center Interconnect (DCI) koppelingen gerealiseerd:

- Gebouwbeveiligingsdienst (ten behoeve van het Facilitair Bedrijf UWV) van Nsecure;
- Capgemini software ontwikkeling en beheer.

De netwerkdiensten van KPN bieden tevens (redundante) netwerkverbindingen en koppelvlakken naar:

- Suwinet/Diginetwerk, ten behoeve van applicatiekoppelingen met SUWI partners en gebruik van UWV-applicaties door Nederlandse gemeentes;
- Belastingdienst, ten behoeve van applicatiekoppelingen;
- Stichting RINIS, ten behoeve van applicatiekoppelingen en toegang tot het internationaal sTESTA netwerk.

Vanuit de centrale firewalls worden diverse IPSEC VPN’s (tunnels) over internet gebruikt naar onder andere Stichting govroam en een overheidsorganisatie.

3.3.4 Internet-breakouts

Er zijn vier centrale internet-breakouts op een veilige wijze gekoppeld aan het netwerk:

1. Werkplek internetverbinding: een generieke KPN werkplek verbinding ten behoeve van het browse verkeer vanuit de fysieke kantoorwerkplekken van UWV en vanuit de virtuele werkplekken van UWV. Tevens wordt deze verbinding gebruikt voor toegang tot de virtuele KPN werkplek voor thuiswerkende UWV-medewerkers;
2. Cloud internetverbinding: internetverbinding die speciek is ingericht voor het gebruik van clouddiensten vanuit de kantoren van UWV, zoals Microsoft Teams / Microsoft 365 en Cisco Webex;
3. Centrale internetverbinding voor het mailverkeer, de ontsluiting van de websites van UWV, internet-verkeer vanuit de applicaties van UWV en vanuit de Wireless LAN’s;
4. Centrale internet-breakout voor Wireless LAN KPN HotSpot met gereguleerde bandbreedte per gebruiker.

Voor specifieke toepassingen worden op enkele kantoren van UWV lokale internetverbindingen op basis van ADSL geleverd. Denk hierbij aan facilitaire meetpunten, een webinarstudio, een evenementenstudio, het test- en securitytestcentrum van UWV en een newsroom van afdeling Communicatie. Deze verbindingen en daarop aangesloten devices zijn volledig geïsoleerd van het UWV LAN/WAN.

3.3.5 Basisdiensten IP

De IP gerelateerde basisdiensten maken integraal onderdeel uit van het netwerk en de KWN-diensten die KPN op dit moment levert. Het betreft de volgende dienstonderdelen:

- Externe DNS-dienst en domein/IP-registrarfunctie, ten behoeve van de DNS-functie voor de internetdomeinen van UWV. De beveiligingsfuncties van deze DNS-dienst (zie paragraaf 3.4.3) voldoen aan de richtlijnen van de overheid;
- Interne DNS-dienst, ten behoeve van de interne domeinen van UWV en de diverse forwarders naar de namespaces die gedelegeerd zijn aan andere gekoppelde ICT-diensten zoals de applicatiedatacenterdiensten van DXC (en Kyndryl);
- Centrale DHCP-dienst, ten behoeve van de diverse IP-scopes van de netwerksegmenten die onderdeel uitmaken van het (Wireless)LAN en WAN;
- IP-adresbeheer, ten behoeve van de adminstratie en uitgifte van IP-subnetten binnen het netwerk van UWV en aangekoppelde ICT-diensten.

Het interne netwerk van UWV en hieraan gekoppelde ICT-diensten maken gebruik van een privaat IPv4 IP-subnet. Op de koppelvlakken met het internet wordt gebruik gemaakt van publieke IP-subnetten van de huidige netwerkleverancier KPN en deels ook van het publieke IPv4 /16 subnet wat eigendom is van UWV.

Vanwege overheidsrichtlijnen wordt op het koppelvlak met internet naast IPv4 ook IPv6 toegepast. UWV heeft daartoe een eigen IPv6-subnet wat voor interne- en externe doeleinden beschikbaar is. Het interne netwerk is wel IPv6 ready maar IPv6 wordt intern niet toegepast.

3.3.6 Interne en externe Mail-relay

Voor SMTP en Secure-SMTP berichtenuitwisselingen via het internet en met ketenpartners biedt het netwerk een externe mailrelay-dienst. Voorbeelden van ketenpartners zijn gemeentes (die samen met UWV de SUWI-wet uitvoeren) en de Belastingdienst. De Mail-relay dienst heeft diverse SMTP-routerings- en beveiligingsfuncties zoals antivirus, antispam en antispoofing (zie paragraaf 3.4.3).

Alle ontvangen en verzonden externe e-mail wordt tevens door de interne mailrelay-dienst afgehandeld. Deze dienst is aangesloten op de Microsoft Exchange-omgeving van UWV en biedt tevens een relay-functie voor applicaties die interne en/of externe e-mail versturen, zoals de fax/scan-dienst en diverse bedrijfsapplicaties van UWV.

Op beide mailrelay-diensten is voor alle e-mail TLS-ondersteuning mogelijk.

3.4 *Securitydiensten*

In deze paragraaf wordt specifiek ingegaan op de securitydiensten die onderdeel zijn van de netwerkdiensten. Dit betreft de security functionaliteit die is geïntegreerd in netwerkdiensten.
Alle in netwerk getroffen security-maatregelen gaan uit van beleidsvoorschriften van de overheid en van UWV. In het algemeen geldt dat UWV de diverse IV-middelen (applicaties, de gegevens die via deze applicaties worden beheerd, netwerkvoorzieningen, eindgebruikers-devices, etc.) classificeert. Deze classificatie wordt gedaan door middel van een risico-impactanalyse aan de hand van de kwaliteitscriteria van informatiebeveiliging: Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV), aangevuld met Controleerbaarheid (C) oftewel aantoonbaarheid (samen BIV-C). De BIV-C classificatie wordt vervolgens gebruikt om te bepalen welke maatregelen benodigd zijn om het gewenste niveau van

beveiliging te realiseren. UWV hanteert daarbij op dit moment maatregelen gebaseerd op de Baseline Informatiebeveiliging Rijksdienst (BIR Tactisch Normenkader (BIR-TNK) en de BIR2012[1]) en overige wet- en regelgeving. De eisen van deze overige wet- en regelgeving komen voort uit de Algemene Verordening Gegevensbescherming (AVG), de Pas toe of Leg uit lijst van Forum Standaardisatie (https://www.forumstandaardisatie.nl) en het Nationaal Cyber Security Centrum (NCSC).
Op dit moment werkt UWV aan de implementatie van de nieuwe richtlijn Baseline Informatiebeveiliging Overheid (BIO). De huidige netwerkleverancier KPN is betrokken bij dit traject.

UWV besteedt veel aandacht aan het verbeteren van het gerealiseerde beveiligingsniveau. De aandacht gaat daarbij in eerste plaats uit naar het borgen van beschikbaarheid, integriteit en vertrouwelijkheid. Daarnaast zijn er specifieke actuele aandachtgebieden, zoals privacy by default, privacy by design, security by design, en het tegengaan van cyberdreigingen. Voor de (huidige en toekomstige) netwerkdiensten gelden zware eisen aangezien de Netwerkdiensten de gehele UWV informatievoorziening bedienen, en UWV met zeer gevoelige data (security en privacy) werkt. Concrete voorbeelden in de huidige situatie zijn: IDS/IPS, malware detectie, web application firewalls, vulnerability scanning, hardening, encryptie op externe- en interne koppelingen en de aansluiting op het Nationaal Detection Netwerk (NDN). De huidige leverancier KPN is daarbij verantwoordelijk voor het bewaken van de netwerkbeveiliging door middel van een eigen Security Operations Center (SOC) en een Security Information and Event Management (SIEM) systeem. Tevens levert KPN loginformatie aan het UWV Security Operations Center (USOC), ten behoeve van concernbrede informatiebeveiliging en SOC/SIEM van UWV.

De securitydiensten die onderdeel uitmaken van de netwerkdiensten vervullen een belangrijke rol in het realiseren van de vereiste beveiligingsniveau's. In de volgende paragrafen wordt nader ingegaan op de functionaliteiten van de belangrijkste securitydiensten binnen het netwerk.

3.4.1 Toegang en segmentatie

De huidige leverancier is verantwoordelijk voor de beveiliging van het netwerk op de grensvlakken met andere netwerken en op de bekabelde- en draadloze toegangen in de kantoren. Om die reden is de toegang tot het kantoornetwerk (LAN en Wireless LAN) beveiligd middels Policy Based Networking (PBN). Zowel op het LAN als Wireless LAN geldt dat alle devices zich eerst dienen te authenticeren voordat het device toegang krijgt tot het juiste netwerksegment. De PBN-dienst is daarom gekoppeld aan de Active Directory van UWV en de Radius Server van govroam.
Een uitzondering vormt de KPN HotSpot-dienst die in de kantoren van UWV ongeauthenticeerde draadloze internet-toegang biedt aan gasten.

LAN en Wireless LAN bieden diverse virtuele netwerken die onderliggend gescheiden zijn op basis van VLAN's of SSID's en de centrale firewalls. Deze virtuele netwerken zijn ten behoeve van:

- Vertrouwde werkplekken van UWV-medewerkers (laptops, dockingstations, desktops, VoIP-telefoons, etc.);
- Internet kiosk werkplekken ten behoeve van klanten van UWV;
- Gebouwbeveiliging met devices zoals tourniquettes, alarmknoppen en camera's (alleen LAN);

[1] ISO 27001 en 27002 zijn opgenomen in de BIR met aanvullingen volgens www.communicatierijk.nl.

- Specifieke andere doelgroepen en functionaliteiten, zoals de afdeling handhaving, printers, testteams, narrowcasting, gebouw- en ruimtebeheer en videoconferencing;
- Bezoekers overheid (govroam);
- Gasten (KPN HotSpot).

Aanvullend ondersteunt het WAN-netwerk vier logisch gescheiden verkeerscategorieën:

- Trusted verkeer, voor UWV-gebruikers, UWV-werkplekdevices, en VoIP;
- Facilitair verkeer, voor facilitaire toepassingen en gebouwbeveiliging;
- Gast verkeer, voor klanten en bezoekers;
- Verkeer ten behoeve van netwerkbeheer.

Deze differentiatie sluit aan op de functionele segmentatie van het LAN en WLAN.

3.4.2 Centrale firewalls

De centrale firewalls zorgen voor de scheiding van de virtuele netwerken. Tevens zorgen deze firewalls voor de vereiste gefilterde connectiviteit naar aanpalende diensten of (externe) netwerken. De centrale firewalls bestaan uit diverse componenten en gelden als centraal koppelpunt voor alle kantoren, ICT-diensten en externe netwerken. Deze dienst wordt de UWV-KoppelDienst (UKD) genoemd. De UKD is volledig redundant uitgevoerd en zorgt voor:

- Zonering en scheiding van de diverse interne virtuele netwerken en aangesloten ICT-diensten en -datacenters. De UKD vormt hierbij het scheidsvlak tussen de interne vertrouwde infrastructuur en de externe wereld. Op deze firewall zijn ondermeer de policies gedefinieerd die de interne communicatiestromen filteren. Daarnaast zijn er policies gedefinieerd voor toegang vanuit/naar het interne netwerk naar/vanuit de externe omgevingen en het internet;
- De "dicht tenzij" grensbewaking tussen het netwerk van UWV en de externe netwerken zoals het internet en het Diginetwerk. Tevens voorziet de UKD in adresvertaling, IPSEC VPN-endpoints, een IDS/IPS-functie en functionaliteit voor IPv6-ondersteuning op het koppelvlak met het internet;
- Demilitarized Zone (DMZ): tussen de interne en de externe firewall bevindt zich een DMZ waar diverse netwerk- en securitydiensten zijn gepositioneerd, voorzover er verkeersstromen tussen de interne en externe wereld worden afgehandeld;
- Veilige koppeling van de diverse aangesloten VoIP SIP-trunks van de huidige leveranciers voor vaste telefonie BT, Vodafone voor mobiele telefonie en Capgemini voor VoIP gerelateerde Contactcenter diensten op het interne netwerk van UWV. Deze koppeling bestaat uit Session Border Controller functionaliteit.

Voorts zijn er firewall-functies actief als onderdeel van de huidige werkplekdienst en de koppeling met Microsoft Teams (zie paragraaf 3.3.4).

De huidige netwerkleverancier is verantwoordelijk voor alle benodigde policies die gerelateerd zijn aan de beveiliging van alle KWN-diensten. UWV toetst deze policies en wijzigingen daarop.
UWV is de aanvrager van functionele policy-wijzigingen. Dit betreft aanvragen gerelateerd aan applicatief verkeer of koppelingen tussen en naar overige aangesloten ICT-diensten. KPN toetst de aanvragen van UWV aan de geldende securityrichtlijnen en zorgt voor de juiste technische implementatie van de policies.

3.4.3 Beveiliging van DNS en e-mail.

De externe DNS-omgeving van UWV (zie paragraaf 3.3.5) voldoet aan de richtlijnen van de overheid, waaronder de richtlijnen genoemd in de 'Pas toe of Leg uit'-lijst van Forum

Standaardisatie (IPV6, DNSSEC). Daarnaast zorgt de DNS-dienst van UWV, in combinatie met de mailrelay-dienst (zie paragraaf 3.3.6), voor adequate beveiliging van de door UWV of partners verstuurde en ontvangen e-mail. Elke e-mail welke uit naam van UWV wordt verstuurd, kan daardoor altijd worden geverifieerd op authenticiteit. Het betreft voornamelijk mechanismes die worden voorgeschreven vanuit de 'Pas toe of Leg uit'-lijst, zoals SPF, DKIM, DMARC, STARTTLS en DANE.

Het UWV Security Operations Center (USOC) monitort en evalueert de effectiviteit van e-mail beveiliging op basis van tooling. Het USOC acteert vervolgens op geconstateerde afwijkingen of misbruik. Deze tooling maakt onderdeel uit van de netwerkdiensten. Het USOC monitort bovendien de correcte implementatie en aanwezigheid van verplichte maatregelen.

Voor de mailrelay-dienst hanteert de huidige netwerkleverancier een beveiligingsbaseline. Deze baseline is in lijn met het UWV-beveiligingsbeleid en de algemene standaarden. Hierin is vastgelegd de veilig beschouwde configuratie, het toegestane gebruik en toegang tot middelen. Hierbij wordt gebruik gemaakt van diverse technieken zoals anti-spam, virusscanning en detectie, filtering van bijlagen, outbreak filters, sender domain reputation detectie en filtering, etc. Wijzigingen worden in overleg met UWV geïmplementeerd. De mailrelay-dienst kent ook een quarantaineomgeving waar verdachte e-mails tijdelijk worden opgeslagen. Gebruikers hebben de mogelijkheid deze e-mails alsnog te lezen of te verwijderen.

3.4.4 Beveiligde internet-toegang

Voor veilige toegang naar of van het internet heeft UWV diverse functies in gebruik:

- De proxydienst ondersteunt het veilig browsen op het internet vanuit de fysieke werkplek op kantoor en de virtuele werkplek. De proxy-dienst filtert URL's op basis van whitelisting, blacklisting, reputatiefilters en controleert en filtert al het verkeer op malware en virussen. Deze dienst biedt daarnaast diverse gebruikersprofielen welke gekoppeld zijn aan autorisatiegroepen. Hiernaast ondersteunt deze dienst vanuit applicaties van UWV geïnitieerde http(s) koppelingen voor bijvoorbeeld webservices van partners;
- Gasten en bezoekers op govroam en KPN HotSpot maken in verband met aansprakelijkheid gebruik van ongefilterd internet. Hierbij is alleen uitgaande initiatie van sessies mogelijk. De centrale firewall (zie paragraaf 3.4.2) zorgt voor de juiste af- en bescherming;
- Ter bescherming van de door publiek en klanten gebruikte websites van UWV wordt een reverse proxy, inclusief web application firewall (WAF) functionaliteit ingezet.
- Alle internet-breakouts van UWV zijn beveiligd tegen DDoS aanvallen.

3.4.5 Overige relevante security-aspecten

Certificaten

UWV maakt gebruik van diverse certificaatverstrekkers ten behoeve van specifieke toepassingen. Te denken valt aan certificaten voor netwerktoegang, site-certificaten voor TLS-beveiliging van publieke websites en servercertificaten voor TLS-beveiliging van koppelingen. Voor koppelingen binnen de overheid wordt gebruik gemaakt van PKIoverheid. Overige certificaten worden uitgegeven door publieke Certificaat Authoriteiten (CA), of de eigen interne CA van UWV. Het beheer van (de lifecycle van) certificaten is binnen UWV centraal belegd. Alle certificaten en gebruikte cipher suites voldoen aan de richtlijnen van het NCSC. De huidige netwerkleverancier KPN onderhoudt de cipher-instellingen.

Identity en Access Management

In de huidige keten wordt wie toegang heeft tot wat voor een belangrijk deel kenbaar gemaakt in het Autorisatie Beheer Systeem (ABS). ABS vertaalt de toegekende autorisaties naar rechtengroepen in de Microsoft Active Directory (AD) van UWV. De AD van UWV heeft een koppeling met de Azure Active Directory (AAD). Bij netwerktoegangscontrole wordt onder andere de AD van UWV ingezet, voor authenticatie van een gebruiker of device. Tevens wordt, voor toegang tot govroam, de authenticatiedienst van Stichting govroam gebruikt.

Remote Access

Zoals vermeld in paragraaf 3.3.4 is er een centrale internet-opgang naar de virtuele werkplek van UWV. Deze opgang maakt het mogelijk voor UWV medewerkers om thuis en onderweg te kunnen werken. Voor het beheren en ontwikkelen van applicaties en overige diensten, is er een separate opgang c.q. opstap voor leveranciers en beheerders. Deze functioneert onafhankelijk van de internet-opgang naar de virtuele werkplek.
Beide toegangen vereisen Multi-Factor-Authenticatie (MFA).

3.5 *Beheerdiensten*

UWV heeft op dit moment het beheer van de huidige netwerkdiensten uitbesteed aan KPN. Onder meer de volgende beheertaken liggen bij KPN:

- Dagelijkse operationele beheerdiensten en monitoring (beschikbaarheid en continuiteit);
- Installeren, beheren en wijzigen van netwerkcomponenten;
- Regiefunctie binnen de netwerkdiensten richting toeleveranciers en fabrikanten;
- Beheer van beveiligingsinstellingen;
- Incident management;
- Problem management;
- Capaciteitsmanagement;
- Wijzigingsbeheer voor standaard en niet-standaard wijzigingen;
- Escalatie management;
- Asset / configuratie management (op basis van een CMDB);
- Security management;
- Life cycle management;
- Service management.

De regieorganisatie van UWV bestuurt en coördineert dagelijks de uitbestede netwerkdiensten. Zij zijn het koppelpunt tussen de vraag van gebruikers en het aanbod van de leverancier. Om de vraag- en aanbodzijde op elkaar af te stemmen worden verschillende overlegvormen gehanteerd. Daaruit voortvloeiende functionele vragen worden door UWV vertaald naar functionele (standaard)wijzigingen en/of projectmatige opdrachten. De leverancier vertaalt deze naar de juiste technische aanpassingen en aanpak.

3.5.1 ITIL-beheerprocessen en proceskoppelvlakken

UWV regisseert de huidige leverancier op basis van ITIL-gebaseerde beheerprocessen (o.a. service level management, incident management, problem management, change management en configuration management) en heeft duidelijke afspraken gemaakt over de proceskoppelvlakken. Als basis geldt de Service Level Agreement (SLA). Voor beschikbaarheid en openstelling van de netwerkdiensten gelden afgesproken service levels. De service levels voor kritische dienstverlening, waarbij redundancy een vereiste is, dienen een uptime-garantie te hebben van 24x7 99.9%. Voor minder kritische dienstverlening

volstaat een uptime van 98.5% tijdens kantooruren (Ma t/m Vrij, 07.00-19.00 uur). De reactie- en hersteltijden van het incidentproces sluiten hierop aan, waarbij het doel is om binnen de overeengekomen SLA de dienstverlening aan UWV te leveren.

Voor de ITIL-beheerprocessen en bijbehorende proceskoppelvlakken gelden afgesproken service levels. De huidige netwerkleverancier rapporteert maandelijks over de gerealiseerde service levels en afwijkingen. Tevens worden specifieke rapportages geleverd over de beschikbaarheid en capaciteit van de diverse netwerkonderdelen. Waar nodig worden verbeteracties gestart om de diensten goed en veilig te laten functioneren. Voor evaluatie van de service levels en de beheerdiensten vinden periodieke overleggen plaats met UWV. Voorbeelden hiervan zijn het service niveau overleg, capaciteitsoverleg en diverse tactische overleggen over het contract, financiele aspecten en vernieuwing van de dienst.

3.5.2 Servicedesk en ITSM

UWV heeft een eigen eerstelijns servicedesk organisatie. Alle service verzoeken, waaronder incidenten en wijzigingsverzoeken voor ICT-diensten en bedrijfsapplicaties, worden hier gemeld. Deze servicedesk routert alle servicecalls naar de diverse oplosgroepen, waaronder KPN als de leverancier van de netwerkdiensten.

KPN heeft een tweedelijns servicedesk die de servicecalls, incidenten en wijzigingsverzoeken vanuit de eerstelijns servicedesk van UWV ontvangt. Indien nodig schakelt KPN door naar derdelijns support van fabrikanten en onderaannemers.
In voorkomende gevallen werkt KPN in het oplossen van incidenten samen met andere ICT-leveranciers van UWV. In geval van complexe en/of kaveloverstijgende incidenten, of bij overschrijding van oplostijden, escaleert UWV naar hogere echelons. Hierbij wordt de coördinatie over het incident door het Keten Regie Loket van UWV overgenomen.

De huidige netwerkleverancier monitort continu de prestatie, capaciteit en beschikbaarheid van de netwerkdiensten en acteert direct op geconstateerde afwijkingen. De beschikbaarheid van de kantoornetwerken wordt gemonitord en via dashboards beschikbaar gesteld aan het Keten Regie Loket van UWV.

Voor automatische doorgifte en uitwisseling van servicecalls zijn de IT Service Management (ITSM) systemen van UWV (Omnitracker) en KPN (ServiceNow) aan elkaar gekoppeld.

3.5.3 BKN en MER/SER beheer

UWV heeft een gecertificeerd bedrijfskabelnetwerk (BKN) inclusief patchpanelen en apparatuurkasten in de kantoren van UWV. In enkele bedrijfsverzamelgebouwen gebruikt UWV de aldaar aanwezige bekabeling van derden.
Elk kantoor kent tevens technische ruimtes, bestaande uit Main Equipment Rooms (MER's) en Satellite Equipment Rooms (SER's). Deze zijn ingericht met klimaat-, brandblus- en noodstroomvoorzieningen, en high availability cabinets (HAC's). UWV is eigenaar van het BKN en alle MER- en SER-voorzieningen. KPN levert en beheert het BKN en de MER- en SER-voorzieningen en heeft onder meer de volgende verantwoordelijkheden:

- IMACD patches / kabels / poorten, op basis van standaard wijzigingsverzoeken;
- Onderhoud en beheer van de MER's en SER's met de daarin aanwezige voorzieningen zoals airco's, UPS'sen en brandblussers. Jaarlijks wordt middels een onderhoudsproject een deel van de voorzieningen vervangen;
- Toegangsbeveiliging van de HAC's in de MER's en SER's;
- Projectmatige levering, aanleg, verwijdering van een BKN en/of MER en/of SER. Dit bij herindeling van kantoorpanden, grootschalige verhuizingen of inrichting van

nieuwe kantoorpanden. Dit wordt gecombineerd met de aanleg van (Wireless)LAN in- en WAN naar de kantoorpanden;
- Bijhouden van een CMDB van de apparatuur in de MER's en SER's en een patch management administratie.

Ter voorbereiding van de aanleg van een BKN in nieuwe kantoren wordt op basis van een blauwdruk, en in samenwerking met het facilitair bedrijf van UWV, de lay-out van het aan te leggen BKN bepaald.

3.5.4 Security management

Security management zorgt ervoor dat wordt voldaan aan de beveiligingsafspraken en aan overige (externe) vereisten, zoals het contract, wet- en regelgeving en (UWV-)beleid. KPN is conform contract verantwoordelijk voor het handhaven en bewaken van deze afspraken en vereisten.

De Security Monitoring Dienst (SOC/SIEM) van KPN monitort de security gerelateerde events binnen de netwerkdiensten op basis van een aantal standaard dreigingsscenario's. Daarnaast worden relevante log-gegevens geautomatiseerd verzameld en via de zogenoemde loghost-dienst doorgegeven aan het UWV-SOC/SIEM-systeem. In het SOC/SIEM van UWV worden de logs afkomstig van alle ICT diensten geaggregeerd en gecorreleerd. Vervolgens worden de logs op basis van (dienstoverstijgende) dreigingsscenario's geanalyseerd door UWV. Het UWV SOC is de eigenaar en bewaker van het UWV-SOC/SIEM-systeem.

KPN draagt daarnaast zorg voor het rapporteren over en het uitvoeren van security management. Dit betekent dat KPN de aanwezige risico's inventariseert, de te nemen mitigerende maatregelen onderbouwt, en de te implementeren oplossingen proactief aanbiedt aan UWV. KPN is in dat kader bijvoorbeeld verantwoordelijk voor het opsporen en verhelpen van kwetsbaarheden. Hiernaast houden zij in- en toezicht op de securitytechnische kwaliteit van de geleverde netwerkdiensten. Tot slot biedt KPN aan UWV een Governance, Risk & Compliance (GRC) dashboard om risico's en operationele compliance te beheren.

3.5.5 Life cycle management

Het Life Cycle Management (LCM) heeft als doel de gecontracteerde functionaliteiten en beveiligingsafspraken over de looptijd van de overeenkomst te kunnen waarborgen. Met behulp van LCM wordt inzicht en advies gegeven over de status van ICT-componenten. Het doel hiervan is het voorkomen van achterstallig onderhoud, onverwachte kosten en onvoorziene beveiligingsrisico's. De huidige netwerkleverancier KPN houdt een roadmap voor LCM bij welke regelmatig met UWV besproken wordt. Daardoor kan tijdig met UWV afgestemd worden wanneer de netwerkleverancier onderdelen gaat upgraden of vervangen. Zodoende worden de netwerkcomponenten up-to-date gehouden. Hierbij worden nieuwe versies van componenten (HW en/of SW) geïmplementeerd en verouderde versies van componenten vervangen en/of uitgefaseerd.

3.5.6 Integratie-, ontwerp-, en adviesdienst

De huidige netwerkleverancier KPN vervult een centrale- en integrale (advies) rol omtrent ontwerp van koppelvlakken met/naar andere partijen toe. Tevens worden ontwerp- en adviesdiensten geleverd op het gebied van nieuwe of aangepaste functionele wensen. KPN werkt onder architectuur en actualiseert de informatieontwerpen en high-level-designs van alle dienstonderdelen. Alle relevante informatie wordt gedeeld met UWV via een daarvoor ingericht informatieuitwisselingsplatform. Voor de doorontwikkeling van de netwerkdiensten biedt KPN een lead-, netwerk-, en security architectfunctie aan. In periodieke overleggen

worden de functionele vragen en benodigde vernieuwingen tussen UWV en KPN besproken. Daarnaast biedt KPN periodiek de roadmap voor netwerkdiensten aan. Daaruit vloeien projectopdrachten voort voor uitbreiding, wijziging en vernieuwing van het netwerk.

Nieuwe koppelvlakken worden op projectmatige basis beschreven, ontworpen en gerealiseerd. Dit in samenwerking met UWV en betrokken externe partijen. Ten behoeve van het facilitair bedrijf van UWV wordt een projectmatige aanpak gehanteerd. Het betreft hier ontwerp en realisatie van de netwerkdiensten (BKN, MER/SER, (Wireless)LAN, WAN) voor nieuwe kantoren of te renoveren kantoren.

3.6 *Koppelvlakken*

UWV heeft diverse externe koppelvlakken in gebruik waarover zij regie voert. Deze koppelvlakken zijn onder te verdelen in de onderstaande categorieën:

1. Externe koppelingen: Integraties met systemen van ketenpartners van UWV, voor applicatietoegang en informatie uitwisseling;
2. Internet-koppelingen: Centrale internet-breakouts (voor werkplek, Microsoft 365, KPN HotSpot en applicatiedatacenters van Kyndryl en DXC);
3. Datacenter-koppelingen: Aansluitingen van functionele koppelvlakken met datacenters voor de werkplek, telefonie, printing, contactcenter, gebouwbeveiliging, en hosting van bedrijfsapplicaties.

Onderstaande Tabel 2 beschrijft de functionele koppelvlakken in meer detail:

Nr.	Kavel/Dienst/Thema	Toelichting
1	UWV-werkplekdienst Virtuele Werkplek UWV – Datacenter koppeling	Koppeling naar KPN-werkplekdatacenters, ten behoeve van toegang vanuit kantoren UWV tot de huidige UWV-werkplekdienst van KPN Werkplek. De UWV-werkplekdienst is volledig gebaseerd op een virtuele werkplek. De migratie naar een Microsoft 365 cloud-gebaseerde Office-functie is in december 2021 gestart.
2	Werkplekdiensten M365 Werkplek UWV – en andere clouddiensten - Internet koppeling	Beveiligd internet-koppelvlak via NL-IX ten behoeve van peer-to-peer koppeling tussen werkplekken op kantoor en Microsoft 365. Daarnaast ook voor koppelvlakken met andere clouddiensten zoals Cisco WebEx.
3	Werkplekdiensten Active Directory – Datacenter koppeling	Koppeling met de on-premises Active Directory voor authenticatiedoeleinden (Policy Based Networking) en autorisatiedoeleinden (proxy-profielen).
4	Telefonie (Huidig, tot eind 2022) – Externe koppeling	VoIP koppelvlak met BT, Vodafone, via een Session Border Controller (SBC). De SBC is onderdeel van de netwerkdiensten.
5	Telefonie (Nieuw, vanaf eind 2022) – Externe koppeling	In de loop van 2022 zal naar verwachting een nieuwe telefonieleverancier worden aangesloten op de bestaande SBC. Het technisch (SIP) koppelvlak blijft gelijk. De telefoniefuncties zullen vanuit een hosted voice oplossing van de opvolgend

Nr.	Kavel/Dienst/Thema	Toelichting
		telefonieleverancier geleverd worden. In het netwerk van UWV blijven VoIP soft- en hardphones gebruikt worden.
6	Contactcenter diensten – Datacenter koppeling	Beveiligd koppelvlak tussen UWV en de Contactcenter diensten, geleverd vanuit twee datacenters van Capgemini. Het netwerk van UWV is via een redundant WAN-koppelvlak aangesloten op deze dienst, ten behoeve van data en VoIP-verkeer. Het VoIP-verkeer wordt ontsloten via de SBC (welke ook voor de telefoniedienst gebruikt wordt).
7	Bedrijfsapplicatie DC Kyndryl t.b.v. interne bedrijfsapplicaties en E-diensten – Datacenter koppeling	Een redundant WAN met de datacenterdienst van Kyndryl. Gedurende 2022 en 2023 worden applicaties gemigreerd naar de DXC-datacenters. Eind 2023, of mogelijk 2024 zal dit koppelvlak naar verwachting worden uitgefaseerd.
8	Bedrijfsapplicatie DC DXC t.b.v. interne bedrijfsapplicaties en E-diensten van UWV – Datacenter koppeling	Een redundant WAN met de datacenterdienst van DXC. In de loop van 2023 zullen de E-diensten via een nieuw beveiligd internetkoppelvlak bij DXC aangesloten gaan worden. Naar verwachting wordt dit eind 2023 afgerond.
9	Printdienst – Datacenter koppeling	Koppelingen tussen Xerox-printerfunctionaliteit op bedraad LAN en de centrale Xerox-printerservers gehost bij KPN. Mogelijk wordt in de loop van 2023 de printdienstverlening opnieuw aanbesteed. Mocht dit het geval zijn, dan zal medio 2024 een nieuw koppelvlak moeten worden ingericht.
10	Derde partijen en (overheids)partners – Externe koppelingen	Beveiligde WAN, VPN en DCI-verbindingen met diverse instanties en derde partijen. Deze verbindingen worden gebruikt voor data-uitwisseling met- en beheeractiviteiten door derde partijen. Hiernaast bieden deze verbindingen toegang tot werkplekfuncties en bedrijfsapplicaties vanuit ketenpartners (SUWI).
11	Internet (filtered) – internet koppeling	Beveiligde koppelingen met het internet ten behoeve van UWV-werkplek browse verkeer en voor bedrijfsapplicaties van UWV voor het kunnen downloaden van diverse software updates.
12	Internet (open) – internet koppeling	Ongefilterde beveiligde koppelingen met het internet ten behoeve van browse verkeer van bezoekers (KPN HotSpot), govroam gebruikers en diverse multimedia-diensten zoals newsroom en studio’s

Nr.	Kavel/Dienst/Thema	Toelichting
13	Internet breakout – KPN HotSpot	Beveiligd internet-koppelvlak van/voor Wireless LAN SSID KPN HotSpot.
14	SOC/SIEM dienst UWV – Datacenter koppeling	Beveiligd koppelvlak met de SOC/SIEM oplossing van UWV, voor beschikbaar stellen van security logging. Alle netwerk logs, maar ook diverse andere logs worden via een centrale loghost van KPN doorgegeven aan het SOC/SIEM-systeem van UWV bij DXC (per februari 2022).
15	NCSC – Externe koppeling	Aansluiting op het Nationaal Detectie Netwerk (NDN) en het Threat Intel Platform (TIP) van het Nationaal Cyber Security Centrum (NCSC) ten behoeve van het monitoren van internet-verkeer.
16	Gebouwbeveiliging – Datacenter koppeling	Koppelen van gebouwbeveiligings-devices op bedraad LAN met het datacenter van de dienst gebouwbeveiliging, via een DCI-koppeling in het datacenter van KPN.
17	Performance & Beschikbaarheidsmonitoring – Datacenter koppeling	Beveiligd koppelvlak voor beschikbaar stellen van event-data van diverse netwerkonderdelen aan de UWV centrale dienst Bedrijfsapplicatieketenmonitoring geleverd door KPN/Measureworks. Dit koppelvlak zal mogelijk wijzigen als gevolg van de aanpassing van de bedrijfsapplicatieketenmonitoringdienst.
18	ITSM-Tooling – internet koppeling	Koppeling tussen UWV's ITSM en de ITSM van de leverancier van de Netwerkdienst, ten behoeve van uitwisseling van servicecalls.

Tabel 2: Beschrijving van de functionele koppelvlakken

3.7 *Lopende projecten*

In onderstaande Tabel **3** staan de reeds lopende, of nog op te starten projecten, die (mogelijk) impact gaan hebben op de huidige en toekomstige Netwerkdiensten:

Nr.	Project	Globale omschrijving	Afronding in:
1	Doorontwikkeling netwerkdiensten	De doorontwikkeling van overige ICT-diensten heeft invloed op de huidige inrichting van de netwerkdiensten. Stapgewijs zullen in de periode 2022-2023 aanpassingen worden doorgevoerd om met name het gebruik van de moderne Microsoft 365 gebaseerde werkplek te kunnen ondersteunen. Dit betreft het project 'Samen naar de Moderne Werkplek" (zie lopende projecten 2022-2024, nr. 4)	2023
2	Migratie Koppelvlak E-diensten	De huidige E-diensten worden ontsloten via de huidige leverancier van de netwerkdiensten. Vanaf 2022 wordt gestart met het migreren en het ontsluiten van alle E-diensten direct via het datacenter van de hosting leverancier DXC. Hierdoor zal de ontsluiting van de E-diensten in de toekomstige situatie (SOLL, per uiterlijk 1/1/2024) geen onderdeel uitmaken van de aanbesteding Netwerkdiensten.	2023
3	Groot onderhoud MER/SER's	Een deel van de MER/SER voorzieningen worden jaarlijks op basis van een onderhoudskalender vervangen, en waar mogelijk aangepast, in verband met afnemend gebruik van de MER/SER ruimtes	2023
4	Herinrichting Werkplek-diensten	Herinrichting werkplekdiensten (programma 'Samen naar de Moderne Werkplek') is volledig gericht op het ontwikkelen van een werkplek gebaseerd op Microsoft 365, en Intune voor device management. Hierbij staat de gebruiker centraal en gaat UWV uit van een 'niet gedeeld en fat' mobiel apparaat. Deze migratie naar een Microsoft 365 werkplek raakt de huidige netwerkdiensten en bepaalt in belangrijke mate de toekomstige netwerkarchitectuur van de aan te besteden Netwerkdiensten.	2024
5	Aanbesteding Werkplekdiensten	Het beheer over de Werkplekdiensten zal aanbesteed worden, waarbij naar verwachting in 2023 de gunning zal plaatsvinden. Mogelijk zullen (nieuwe) technische en of functionele koppelvlakken met de Netwerkdiensten moeten worden ingericht of herzien.	2024
6	Aanbesteding en herinrichting Telefoniediensten	De huidige situatie op het gebied van telefonie wordt gekenmerkt door een scheiding van mobiel, vast en werkplek. Telefonie wordt in 2022 aanbesteed en zal mogelijk de huidige en toekomstige situatie van Netwerkdiensten raken door nieuwe of aangepaste koppelvlakken voor vaste telefonie (VoIP).	2023
7	Transitie datacenters Kyndryl naar DXC	UWV is momenteel bezig met de transitie van bedrijfsapplicaties van Kyndryl datacenters naar DXC datacenters. In de loop van 2023, of mogelijk 2024,	2024

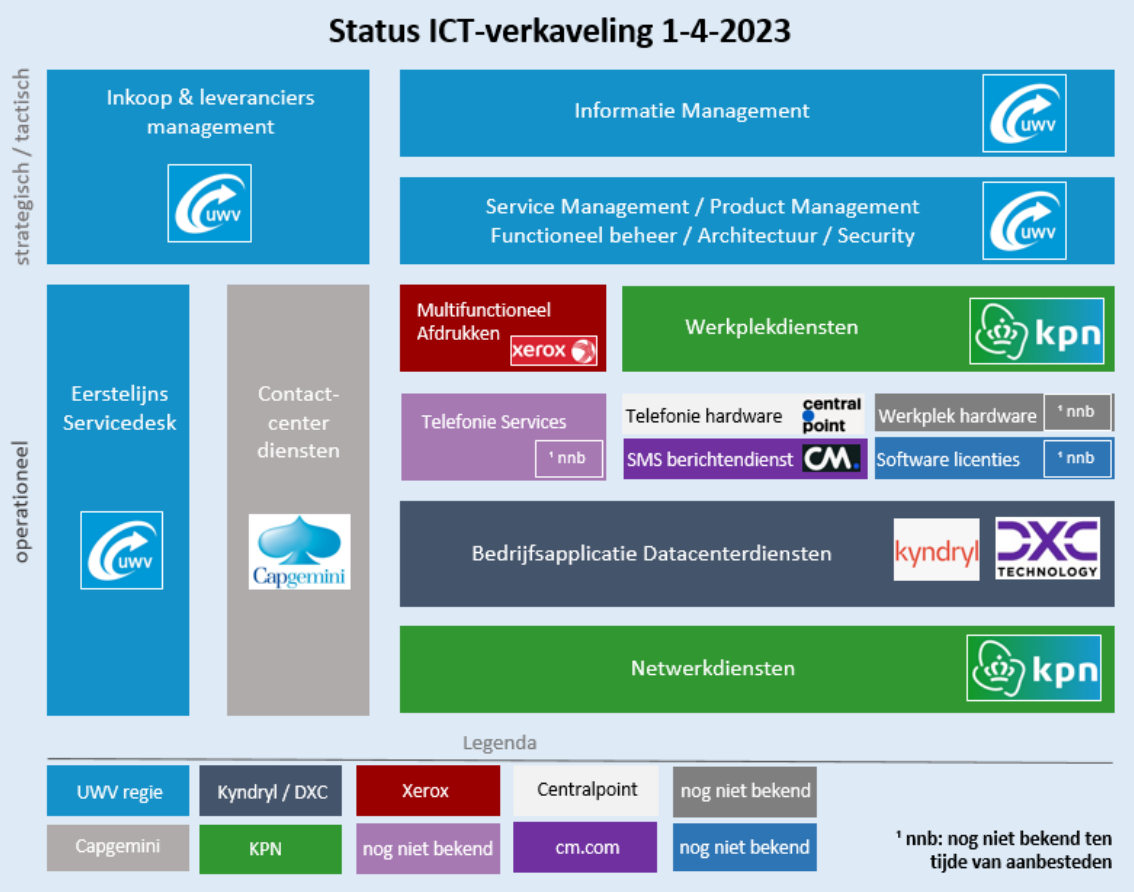
Nr.	Project	Globale omschrijving	Afronding in:
		zullen alle functionele koppelingen gemigreerd zijn naar DXC. Tevens worden de WAN-verbindingen tussen Kyndryl en DXC uitgefaseerd.	
8	Aanbesteding Contactcenter diensten	UWV zal in de loop van 2024 starten met het aanbesteden van de contactcenter diensten van het klant contact centrum van UWV. De uiteindelijke oplossing heeft invloed op technische en functionele koppelvlakken van de Netwerkdiensten en mogelijke LAN/WAN inrichting.	Start 2024 t/m 2025
9	Aanbesteding dienst Multifunctioneel afdrukken	UWV zal mogelijk in de loop van 2023 starten met het aanbesteden van de Print/Scan/Fax/Kopier-dienst. De uiteindelijke oplossing heeft invloed op technische- en functionele koppelvlakken van de Netwerkdiensten en mogelijk de LAN/WAN- inrichting.	Start 2023 t/m 2024
10	Herinrichting Identity en Access Management (Programma Helios)	UWV is bezig met herinrichting van het Identity en Access Management & Governance (IAM&G) landschap. Het huidige AutorisatieBeheer Systeem (ABS) zal vervangen worden door een andere oplossing. De directory services zullen vanuit deze nieuwe oplossing geprovisioned worden met identities en autorisaties. Met name zal dit attribute based access mogelijk gaan maken	2024
11	Next Level Security	Project Next Level Security. Detaillering volgt in de Uitnodiging tot Inschrijving (UtI).	2023

Tabel 3: Lopende projecten

4. Beschrijving toekomstige situatie

4.1 *ICT-landschap UWV 2023-2024*

In de vastgestelde sourcing strategie is gekozen voor een verkaveling waarbij de KWNTC-diensten verder worden opgesplitst dan in de huidige situatie het geval is. Deze splitsing is inzichtelijk gemaakt in Figuur 4. Voor de Netwerkdiensten betekent dit dat deze diensten separaat worden aanbesteed.



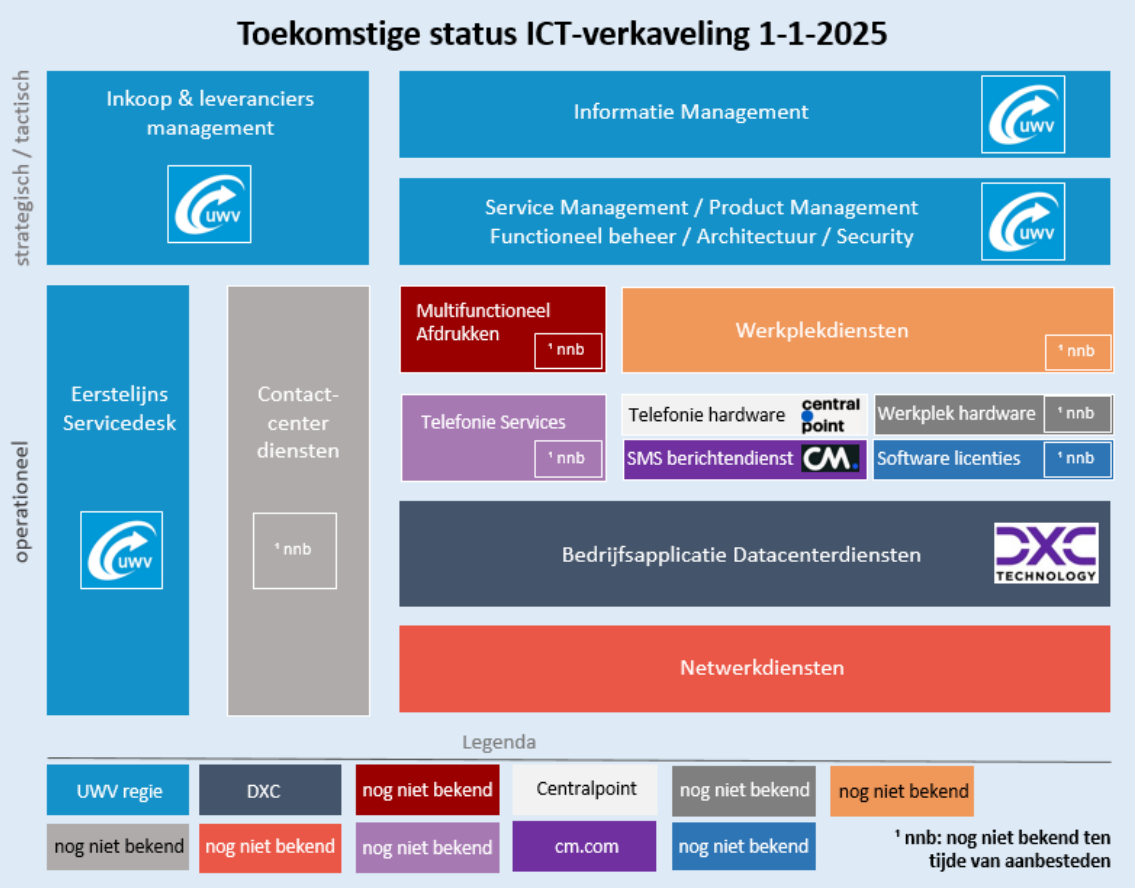
Figuur 4: Status ICT-verkaveling 1-4-2023

Zoals in Figuur 4 is weergegeven, worden meerdere diensten opnieuw aanbesteed. Momenteel is nog niet bekend (nnb) welke leveranciers daarvoor geselecteerd worden. Conform de KWNTC-visie van UWV op het aspect sourcing gaat de invulling van die kavels veranderen ten opzichte van de huidige situatie. Dit heeft effecten op de Netwerkdiensten.

Naar verwachting ontstaat vanaf medio 2022 binnen de huidige KPN werkplekdienst een hybride kavelinvulling. De hybride werkplekdienst bestaat uit de doeloplossing Microsoft 365 en 'legacy diensten' van KPN (waaronder de virtuele werkplek). Deze ontwikkeling loopt nagenoeg parallel aan de aanbestedingen van de Werkplek- en Netwerkdiensten. Zowel in de transitie als daarna zullen de Werkplek- en Netwerkdiensten goed op elkaar moeten blijven aansluiten.

In onderstaande Figuur 5 wordt een indicatie gegeven van de situatie na de transitie van de Netwerkdiensten (begin 2025). Vermoedelijk is rond die tijd de aanbesteding van de printdienst bezig, of al afgerond. Tevens loopt in die periode de aanbesteding van de

Contactcenter diensten. Daarnaast zal dan naar verwachting de Datacenter transitie van Kyndryl naar DXC zijn afgerond.



Figuur 5: Toekomstige status ICT-verkaveling – begin 2025

Figuur 1, Figuur 4 en Figuur 5 laten zien dat het ICT-landschap de aankomende jaren, van begin 2022 tot begin 2025, onderhevig is aan grote veranderingen. Deze veranderingen zorgen voor extra complexiteit binnen de huidige en toekomstige Netwerkdiensten. De meeste kavels zullen in de periode tot begin 2025 zijn gegund en opnieuw worden ingericht. Ten opzichte van 'Figuur 4: Status ICT-verkaveling 1-4-2023' zullen ook de kavels Netwerk- en Werkplekdiensten gegund zijn. Voor Werkplekdiensten zal dit betekenen dat naar verwachting in 2023 Microsoft 365 als dienst (deels) is uitgerold. De inrichting van Netwerkdiensten zal hier functioneel en technisch op moeten aansluiten, om zo Werkplekdiensten en alle overige kavels op de gewenste wijze te kunnen faciliteren. De ingerichte Netwerkdiensten zullen uitgerold zijn op basis van de in dit hoofdstuk beschreven toekomstige situatie.

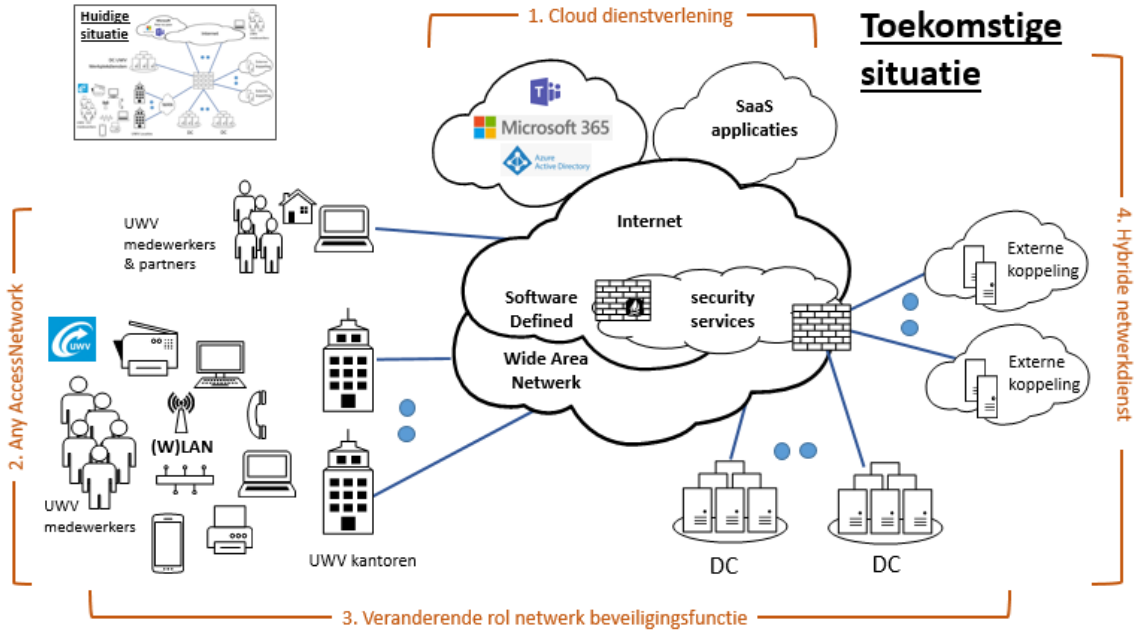
4.2 *Visie, doelstellingen en principes*

4.2.1 Visie

Op het gebied van werkplekinrichting en applicatieontsluiting zien we de komende jaren grote veranderingen. Veranderingen waar de netwerkinrichting continue op zal moeten blijven aansluiten. Deze veranderingen zijn dan ook de aanjagers ('Drivers of Change') van de transformatie naar de toekomstige netwerkinrichting. Binnen de Netwerkdiensten zien we de volgende belangrijkste 'Drivers of Change':

1. Cloud dienstverlening;
2. Any AccessNetwork;
3. Geïntegreerde rol van de netwerkbeveiligingsfunctie;
4. Hybride Netwerkdiensten.

Onderstaande Figuur 6 geeft een globaal overzicht van de verandering van het netwerk ten opzichte van de in Figuur 3 weergegeven huidige situatie. De Netwerkdiensten bevinden zich in een wisselend en breed speelveld. Aangepaste functionaliteiten en nieuwe eisen en wensen vanuit de bedrijfsvoering jagen veranderingen in de bestaande Netwerkdiensten aan.



Figuur 6: Globale weergave van de toekomstige situatie van het UWV-netwerk

De 4 genoemde 'Drivers of change' worden hieronder nader toegelicht:

1) Cloud dienstverlening; van on-premises applicatieontsluiting naar cloud-applicaties:
Het kunnen ondersteunen van cloud-gebaseerde samenwerkingsfuncties stelt hogere eisen aan bandbreedte, latency, beveiliging, flexibiliteit en schaalbaarheid. Een aantal eindgebruikersdiensten dat UWV afneemt, dan wel gaat aanbesteden, wordt uit de (public) cloud afgenomen. Dit geldt onder andere voor de Microsoft 365 werkplek, de "Hosted Voice" Telefoniedienst en de Contactcenter diensten. De functionaliteiten van deze cloud-diensten stellen hoge eisen aan het netwerk. Daarnaast worden deze diensten rechtstreeks vanuit de eindgebruiker-devices benaderd en niet meer vanuit een hosted virtuele werkplek. De Netwerkdiensten zullen de vereiste veilige koppelvlakken met de nieuwe (public)cloud-diensten moeten ondersteunen.
UWV is bezig met het actualiseren van het UWV cloudbeleid, gericht op het in lijn brengen met het cloudbeleid van CIO Rijk, dat in 2022 verruimd lijkt te worden. Dit geactualiseerde UWV cloudbeleid zal van toepassing zijn op alle clouddiensten, ook netwerk en securitydiensten, die op basis van public cloud worden gecontracteerd. Zolang het geactualiseerde UWV cloudbeleid niet is vastgesteld, zal er getoetst worden op basis van toegevoegde waarde (op het vlak van onder andere kosten, functionaliteit, flexibiliteit, veiligheid, schaalbaarheid, retransitie) van een public cloud oplossing ten opzichte van een on-premises oplossing. Tevens maakt een risicoanalyse onderdeel uit van het toetsen van de oplossing.

2) Any AccessNetwork; mobiel werken vanaf elke plek op elk mogelijk tijdstip:
Eindgebruikers van UWV zijn, mede ingegeven door de Covid-pandemie, steeds meer vertrouwd geraakt om te werken vanaf elke locatie en op elk moment. Deze manier van werken is sinds begin 2020 aanzienlijk toegenomen. Echter in de huidige situatie zijn de Netwerkdiensten hoofdzakelijk ingericht ter ondersteuning van een thin-client (Server Based Computing (SBC)) werkplekarchitectuur. In de toekomstige situatie zullen de Netwerkdiensten zo ingericht moeten zijn dat deze de nieuwe Moderne Werkplek kunnen faciliteren.

Het werken vanaf elke locatie en elk moment betekent dat er minder zicht is op de daarvoor gebruikte netwerken en het ingestelde beveiligingsniveau. Door het werken met een internet-centrische werkplek in de public cloud is er minder grip en controle. Met name toegang (zero-trust), veiligheid en performance wijkt hiermee af van de traditionele netwerkinrichting. Dit vormt een risico voor de on-premises en public-cloud applicaties met gevoelige informatie. Om deze reden is een aanpassing van de netwerkbeveiligingsfunctie- en toegangsoplossingen vereist, meer gebaseerd op een zero-trust-aanpak.

3) Geïntegreerde rol netwerkbeveiligingsfunctie;
De verschuiving van network-based naar identity-based werken, volledig onafhankelijk van tijd en locatie, zal andere eisen stellen aan de inrichting van de netwerkbeveiligingsfunctie:

- Strikte identiteit –en systeemverificatie wordt een vereiste voor alle gebruikers en systemen. Dit geldt voor zowel toegang tot het netwerk als toegang tot alle aangesloten diensten. Toegangscontrole vindt op een need-to-use basis plaats en toegangsrechten worden op basis van mate van vertrouwen verleend;

- De netwerkbeveiligingsfuncties gaan een integraal onderdeel uitmaken van de toekomstige Netwerkdiensten. Hierbij zullen technologiën waaronder SD-Wan, Cloud Security en Security Services integreren met de netwerktransportfunctie. Hierbij worden gebruikers en systemen geïdentificeerd, wordt beleid gebaseerde beveiliging toegepast en wordt gecontroleerde toegang tot de juiste applicaties of gegevens geboden.

4) Hybride Netwerkdiensten;
De aan te besteden Netwerkdiensten ondersteunen de omslag van kantoor gebaseerd werken naar werken vanaf elke locatie. Concreet betekent dit ondersteuning van de omslag van het werken binnen een veilig netwerk met on-premises diensten naar meer cloud gebaseerde diensten “Anywhere” (thuis, onderweg, op kantoor). Deze geleidelijke omslag vindt de komende jaren plaats. Daarbij dienen on-premises diensten zeker de komende periode ook nog veilig ontsloten te worden. Het toekomstige netwerk zal dan zowel de nieuwe ontwikkelingen (cloud diensten) en de huidige omgevingen (on-premises applicaties en diensten) moeten faciliteren.

4.2.2 Doelstellingen

Een beschrijving van de doelstellingen voor de toekomstige Netwerkdiensten staat beschreven in de Uitnodiging tot Aanmelding (UtA): Paragraaf 3.2 “doelstellingen van de opdracht”.

4.2.3 Principes

De toekomstige situatie is gebaseerd op de onderstaande principes:

1) WiFi-toegang tenzij:
Het principe WiFi-toegang tenzij richt zich op flexibel werken binnen de kantoren van UWV door middel van draadloze toegang tot het netwerk. Dit geldt voor de verschillende interne en externe netwerk gesegmenteerde doelgroepen. Medewerkers zijn voorzien van een laptop en smartphone en moeten hun werk flexibel vanaf elk UWV kantoor kunnen uitvoeren. Voor bezoekers en klanten wordt een gescheiden WiFi-toegang tot internet geboden. Voor bepaalde devices waaronder vaste werkplekken, Access Points, IOT-legacy devices, gebouwbeheer devices zal bedrade netwerkconnectiviteit worden geboden.

2) 'Anywhere-access', tenzij:
Onafhankelijk van de locatie waar zij werken, hebben medewerkers van UWV een uniforme beveiligde toegang tot internet, cloud-diensten en bedrijfsapplicaties nodig. Deze toegang biedt onder andere een authenticatie-, inspectie-, en preventie-laag en zorgt voor de beveiliging van UWV-tenants in de cloud en voor beveiligde toegang tot (legacy) bedrijfsapplicaties in het datacenter. Gebruikers en systemen dienen op basis van hun locatie, device en individuele identiteit vooraf voor de dienst geauthenticeerd en geautoriseerd te zijn.

3) *Identity-based toegangsbeleid, tenzij*:
De zero-trust identity-based beveiligingsinrichting richt zich op de identiteit en beveiligingsstatus van gebruikers, devices en applicaties. Toegang tot resources wordt alleen verkregen op basis van de validatie van de gebruikersidentiteit, het aanwezige toegangsrecht en de status van het device. Dit met als doel om de kans op aanvallen te verkleinen. Daarnaast moeten alle netwerkactiviteiten worden gecontroleerd op bedreigingen, ook na autorisatie en het leggen van een verbinding met geprivilegieerde bronnen. Waar de identity-based inrichting (vooralsnog) niet implementeerbaar is, wordt teruggevallen op het huidige netwerk-based toegangsbeleid, mogelijk aangevuld met extra maatregelen.

4.3 *Scope van de aanbesteding Netwerkdiensten*

De aan te besteden Netwerkdiensten ondersteunen de in de vorige paragrafen beschreven visie. Dit betreft Anywhere veilige, en beveiligde toegang tot private en public cloud applicaties en internet. Hierbij gaat het toegangsbeveiligingsniveau uit van het zero-trust principe. Delen van de netwerk- en securityfunctionaliteit zullen steeds meer via internet beschikbare "as a service"-diensten worden afgenomen. Andere delen van het netwerk zullen ter ondersteuning van bestaande (legacy) toepassingen traditioneel in/tussen kantoren als besloten dienst worden afgenomen. Deze hybride situatie is een uitgangspunt voor de aanbesteding Netwerkdiensten. In deze aanbesteding maken de beveiligingsfuncties, naast de transportfuncties, een belangrijker en meer geïntegreerd onderdeel uit van de Netwerkdiensten dan voorheen.

Het belang van de Netwerkdiensten is groot: UWV heeft een vitale functie in de samenleving en is voor de uitvoering van haar taken sterk afhankelijk van de goede werking en beschikbaarheid van de ICT infrastructuur. Opdrachtnemer dient dit belang dus op de juiste wijze in ogenschouw te nemen.

De volgende paragrafen beschrijven de scope van de aan te besteden Netwerkdiensten, bestaande uit:

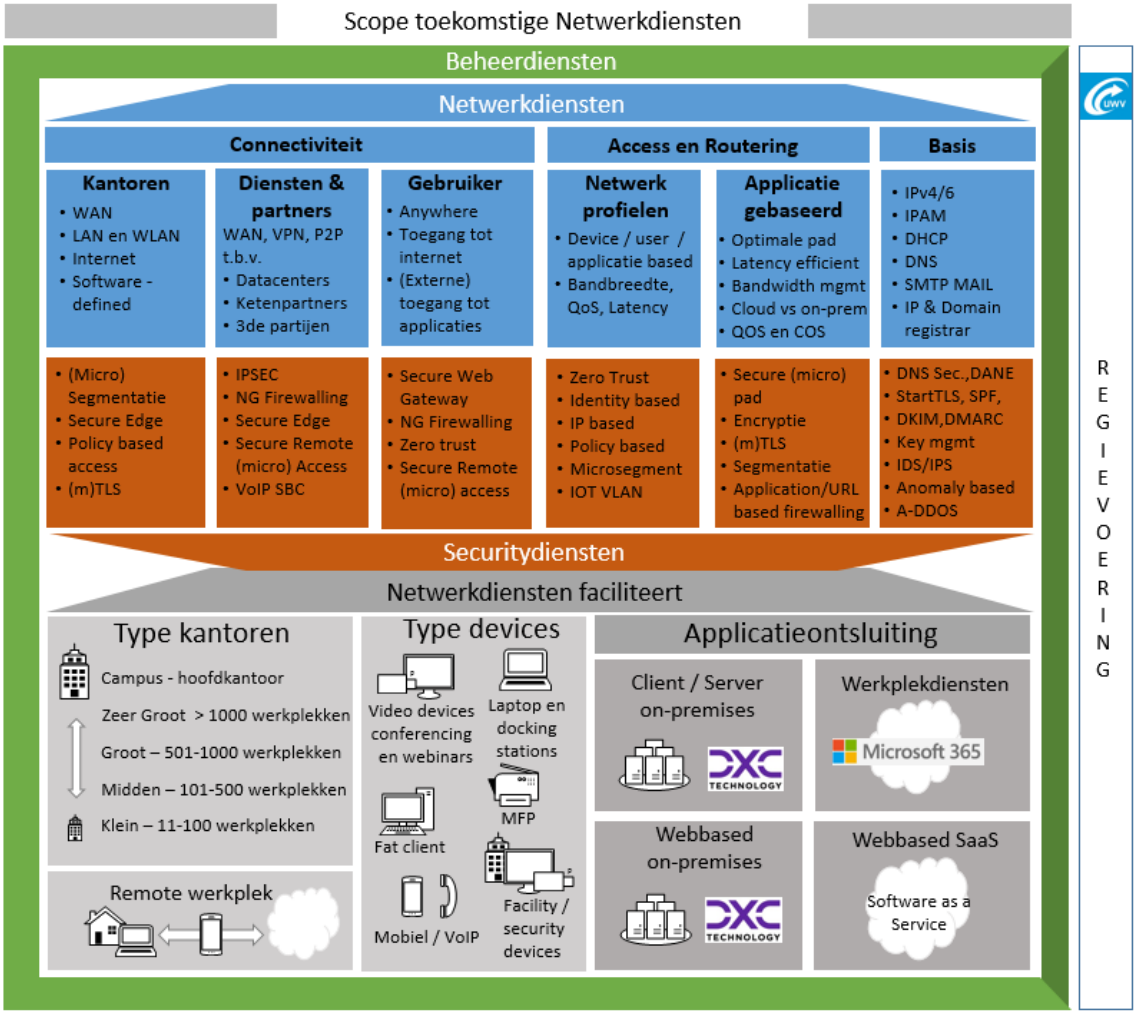
- Basis netwerkdiensten (paragraaf 4.4);
- In Netwerkdiensten geïntegreerde securityfuncties (paragraaf 4.5);
- Benodigde beheerdiensten (paragraaf 4.6);
- Koppelvlakken met andere ICT diensten en partners (paragraaf 4.7);
- Transitie van de huidige naar de nieuwe leverancier en transformatie (paragraaf 4.8).

Tot slot wordt ingegaan op de diensten die optioneel in scope zijn (paragraaf 4.9) en de diensten die niet meer in scope zijn (paragraaf 4.10).

Voor de geschetste scope zijn de volgende punten nog van belang:

- UWV sluit niet uit dat onderdelen van de Netwerkdiensten in de toekomst via overheidsbrede dienstverlening zullen worden afgenomen. Eventueel benodigde ontwerp-, integratie-, migratie- en beheeractiviteiten voor aansluiting op die overheidsdienstverlening zullen mogelijk bij Opdrachtnemer worden belegd;
- De Netwerkdiensten maken het mogelijk om thuis te kunnen werken. Binnen UWV is er nog geen besluit genomen of de hiervoor benodigde thuisvoorzieningen (WiFi, ADSL, etc) via de onderhavige aanbesteding verworven zullen worden;
- Het kantoornetwerk van Bureau Keten Werk en Inkomen (BKWI) is momenteel geen onderdeel van het huidige netwerk. UWV zal tijdens de UtI-fase bepalen of het betreffende kantoor van BKWI op het UWV netwerk zal worden aangesloten.
- UWV sluit niet uit dat een aantal direct aan Netwerkdiensten gerelateerde technische en facilitaire zaken gedurende de looptijd van de Overeenkomst bij Opdrachtnemer zullen worden afgenomen.

Onderstaande Figuur **7** toont een eerste aanzet van de mogelijke invulling van de toekomstige Netwerkdiensten. Het betreft de netwerk-, security- en beheerdiensten alsmede de diensten, devices en kantoren die vanuit Netwerkdiensten worden gefaciliteerd.



Figuur 7: Globaal overzicht van de toekomstige Netwerkdiensten.

4.4 *Basis netwerkdiensten*

Tot de scope van de aanbesteding Netwerkdiensten behoren de Basis netwerkdiensten. Deze diensten hebben betrekking op connectiviteit en transport van data en zijn in te delen in tenminste de volgende onderdelen:

1) Connectiviteit voor kantoren van UWV:
De Opdrachtnemer levert bedraad en draadloos lokaal netwerk (LAN en Wireless LAN) in alle kantoren van UWV. Het (W)LAN dient aangesloten op- en geïntegreerd te worden met een software bestuurde Wide Area Network (WAN) oplossing. De kantoornetwerken bieden connectiviteit naar alle aangesloten ICT-diensten (zoals de bedrijfsapplicatie Datacenterdiensten) van UWV. Tevens is er voor de kantoornetwerken een zo kort en snel mogelijk pad naar internet met voldoende bandbreedte beschikbaar. Dit ten behoeve van het gebruik van public cloud-diensten zoals Microsoft 365, diverse multimedia toepassingen, en toegang tot internet voor gebruikers en gasten. Alle kantoornetwerken zijn afdoende beveiligd op het scheidingsvlak (Edge) richting internet. De opdrachtnemer maakt, op basis van de door UWV gestelde beschikbaarheids-, veiligheid-, en performance eisen, onderbouwde keuzes voor type transportverbindingen en gebruikte technologie.
Voor hele specifieke toepassingen kan een separate geisoleerde internet verbinding (DSL) vereist zijn.

2) Connectiviteit van aangesloten diensten en partners:
De Opdrachtnemer levert (IPSEC) VPN en WAN verbindingen voor de netwerkaansluiting van (keten)partners en datacenters van overige ICT-kavels.

3) Connectiviteit voor externe toegang:
De Opdrachtnemer levert externe toegang (o.a. netwerkpaden, bandbreedte) voor UWV-gebruikers die vanuit thuis of onderweg on-premises applicaties van UWV willen gebruiken. Tevens wordt externe toegang geboden aan gebruikers van derde partijen met eigen werkplek-devices. Denk hierbij aan gebruikers die beheerwerkzaamheden op on-premises ICT-systemen uitvoeren.

4) Netwerkprofielen:
De Opdrachtnemer levert netwerkprofielen per aangesloten dienst in combinatie met de op het netwerk aan te sluiten (type) devices. De profielen sluiten aan op de capaciteits-, kwaliteits- en beveiligingsvereisten van de diverse verkeersstromen. Onder meer betreft het profielen voor:

- UWV-werkplekken (Microsoft 365) met toegang tot interne bedrijfsapplicaties en public cloud-applicaties;
- VoIP telefonie;
- Internet gastgebruik;
- Video vergaderen;
- Narrowcasting;
- Gebouwbeheer;
- Gebouwbeveiliging;
- Printers.

De profielen worden bij aansluiting/onboarden van devices zoveel mogelijk automatisch toegekend. Eindgebruikers kunnen met werkplek-devices eenvoudig onboarden op de voor UWV-werkplekken bestemde profielen. Het bedrijfsbreed toevoegen, veranderen of verwijderen van profielen dient eenvoudig te worden gerealiseerd via centrale software-gebaseerde besturing.

5) Applicatie gebaseerde routering:
De Opdrachtnemer levert de meest optimale route per applicatie of groep van applicaties. De optimale route hangt af van de capaciteits- performance- en beveiligingseisen van applicaties. Bijvoorbeeld: Een Microsoft Teams video-sessie op kantoor volgt op basis van latency en bandbreedte-eisen een andere route dan een geraadpleegde willekeurige website of bedrijfsapplicatie.

6) Basis netwerkfuncties:
De Opdrachtnemer levert essentiële basisfuncties zoals

- IP V4/V6 registratie, administratie en uitgifte voor het gehele netwerk (inclusief uitgifte van subnetten voor aangesloten ICT leveranciers);
- DHCP;
- Interne- en externe DNS;
- IP- en domain-registrar;
- Interne- en externe SMTP-mailrelay, mogelijk in combinatie met Microsoft 365;
- Generatie, uitgifte en beheer van beveiligingssleutels voor bijvoorbeeld (m)TLS, waar mogelijk gebaseerd op een geautomatiseerde oplossing.

De bovenstaande netwerkfuncties dekken de volgende capaciteits-, kwaliteits-, en beschikbaarheidsaspecten af:

- Geboden capaciteit, routepaden en latency voldoen ten minste aan de richtlijnen die gelden voor Microsoft 365. Hiernaast zijn deze flexibel ingericht voor gebruik van andere toekomstig aan te sluiten public cloud-diensten;
- De netwerkdiensten zijn schaalbaar met waar mogelijk automatische op- en afschaling;
- De capaciteit en kwaliteit van (Wireless)LAN- en WAN maakt breed gebruik van videobellen, videoconferencing, VoIP, webinars, en live video events mogelijk;
- De Netwerkdiensten zijn 24x7 operationeel en waar nodig redundant uitgevoerd;
- Voor kantoornetwerken en koppelingen met (keten)partners en andere ICT-diensten worden verschillende beschikbaarheidsniveaus gehanteerd. De vereiste beschikbaarheid hangt af van het type gebruik, omvang en belang van het kantoor of de koppeling;
- Te allen tijde dient UWV haar kerntaken uit te kunnen voeren en dienen de primaire bedrijfsapplicaties toegankelijk te zijn. De Netwerkdiensten bieden daarom een fallback-oplossing ten behoeve van vitale UWV-functies. Dit in geval van uitval of afsluiting van bijvoorbeeld het internet-pad of “as a service” gebaseerde netwerkfuncties.

4.5 *Securitydiensten*

De dienstverlening van UWV is van vitaal belang voor het maatschappelijk verkeer in Nederland. De continuïteit en veiligheid van de informatievoorziening voor operationele processen moet daarom verzekerd zijn. UWV verwacht dat de Opdrachtnemer van de Netwerkdiensten het juiste niveau van informatiebeveiliging en infrastructuurbescherming levert. Hiermee wordt de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van de informatievoorziening conform eisen en wensen van UWV gerealiseerd. De securityfuncties van de Netwerkdiensten stellen UWV in staat om haar informatievoorziening preventief te beveiligen. Deze securityfuncties dienen zoveel mogelijk geïntegreerd te zijn met de in paragraaf 4.4 beschreven connectiviteits- en transportfuncties.

De volgende securityfuncties maken ten minste onderdeel uit van de scope van de opdracht:

1) Toegangcontrole:
Op het (Wireless)LAN kantorennetwerk en alle koppelvlakken tussen en naar internet, (keten)partners, overheidsnetwerken en datacenters wordt de toegang gereguleerd. De toegangscontrole kan zich op meerdere punten in het netwerk bevinden en vindt plaats op basis van identiteit en/of netwerkkenmerken. Uitgangspunt hierbij is dat devices en gebruikers als niet-vertrouwd worden beschouwd. Toegang tot het UWV-netwerk en aangesloten ICT-diensten wordt verstrekt op basis van het least-privilige principe.
De netwerktransitie mag geen impact hebben op de huidige gekoppelde ICT-diensten en (keten)partners, waar veelal gebruik wordt gemaakt van toegangscontrole op basis van netwerkkenmerken. Zodoende blijven een aantal traditionele netwerken voldoende afgeschermd. Afhankelijk van mogelijke dreigingen op een koppelvlak is de toegangscontrole versterkt met intrusion-detection en intrusion-prevention mechanismes. UWV verwacht wel dat gedurende de looptijd van het contract de op identiteit gebaseerde toegangscontrole de standaard wordt en toegangscontrole op basis van netwerkkenmerken gaat afnemen.
De policies die gehanteerd worden bij toegangsverstrekking aan gebruikers zijn gebaseerd op de policies in de UWV Identity- en Accessmanagement (IAM) omgeving. Hier worden de identities en de autorisaties voor gebruik van ICT-diensten en bedrijfsapplicaties beheerd.

2) Beveiligingsprofielen (onderdeel van netwerkprofielen):
Zoals in paragraaf 4.4 staat beschreven, worden op- en tussen de kantoornetwerken netwerk-profielen gehanteerd voor de diverse type devices, gebruikers en toepassingen. Deze profielen reguleren integraal de logische (micro)segmentatie van het netwerk, zodat onder andere afscherming van meer besloten ICT-diensten mogelijk is. Dit op basis van policy-based netwerktoegang. De benodigde beveiligingsmaatregelen zijn zoveel mogelijk integraal onderdeel van het netwerkprofiel en voorkomen onnodig oost-west-verkeer op segmenten. Idealiter wordt microsegmentatie toegepast.

3) Veilige toegang tot internet:
De Netwerkdiensten bieden overal een veilige toegang tot internet voor eindgebruikers met een UWV-werkplek. De UWV-werkplek dient goed beschermd te zijn tegen dreigingen.
De veilige internet-toegang (web-gateway) biedt onder meer een proxy-functie, een anti-virus/malware-filter, en een URL-filter (blacklisting/whitelisting/reputation). De web-gateway ondersteunt verschillende profielen voor bijvoorbeeld beperkt gebruik, standaard gebruik en uitgebreid gebruik. De voor de profielen benodigde autorisaties zijn gebaseerd op de IAM-rollen van UWV. Idealiter zijn deze profielen geïntegreerd met de in paragraaf 4.4 genoemde netwerkprofielen. De web-gateway is overal bereikbaar, via de internet-aansluiting thuis, onderweg of op kantoor. De web-gateway-functie wordt niet gebruikt om gasten op het UWV-Wireless LAN toegang te bieden tot internet. Zij maken gebruik van ongefilterd internet, op basis van de juridische voorwaarden bij het gebruik van de dienst. Voor specifieke netwerkprofielen ten behoeve van videoconferencing, webinar feeds, event studio, en de newsroom videowalls is veilige toegang tot internet wel van belang. De vereiste protocollen dienen goed ondersteund te worden.

4) Veilige toegang tot (public) cloud-diensten (SaaS) en on-premises applicaties;
De Netwerkdiensten bieden overal (Anywhere) een veilige toegang tot public cloud, SaaS en on-premises bedrijfsapplicaties voor eindgebruikers met een UWV-werkplek en beheerders/gebruikers van derde partijen. Deze functie zorgt voor gecontroleeerde toegang tot de door UWV en derden gebruikte applicaties door middel van identity- en risk-based policies.

UWV maakt gebruik van circa 400+ applicaties. Microsoft 365 functionaliteit wordt op het werkplek-device van de UWV-gebruiker beschikbaar gesteld. Deze Moderne Werkplek zal de komende jaren een steeds belangrijkere rol gaan spelen in de beschikbaarsteling van de applicaties. Het gebruik van de huidige virtuele werkplek gaat steeds meer afnemen. Ten aanzien van de veilige toegang tot cloud-diensten en applicaties zijn de volgende ontwikkelingen te verwachten:

- Microsoft 365 applicaties en moderne standaard applicaties (native apps) worden op UWV-werkplek-devices beschikbaar gesteld en worden via Microsoft Intune direct vanaf internet geüpdatet. Sterke authenticatie vindt plaats op basis van Microsoft Azure Active Directory (AAD). Deze AAD van UWV wordt gesynchroniseerd met de on-premises Active Directory van UWV. Mogelijk wordt de AAD ook geprovisioned vanuit een toekomstig nieuw autorisatiebeheersysteem van UWV. Het UWV-werkplek-device is vanuit de kavel Werkplekdiensten voorzien van een continue actuele en actieve endpoint protection, mogelijk aangevuld met een Endpoint threat Detection and Response (EDR) oplossing.
- UWV gebruikt steeds meer webbased SaaS-applicaties van vele aanbieders. Authenticatie wordt daarbij momenteel gerealiseerd middels de on-premises Active Directory Federation Services (ADFS) identity Provider (IdP) waardoor Single Sign On (SSO) mogelijk is. De IdP dwingt tevens Multi Factor Authenticatie (MFA) af. De authenticatie zal verschuiven naar moderne authenticatie en federatie op basis van

Microsoft AAD. De applicaties zullen rechtstreeks vanuit de browser van het UWV-werkplek-device gebruikt gaan worden. De browser wordt onder regie van Microsoft Intune direct vanaf internet geüpdate.

- De webbased on-premises UWV bedrijfsapplicaties, gehost in de on-premises datacenters, zullen steeds meer rechtstreeks vanuit de browser op het UWV-werkplek-device gebruikt gaan worden. Authenticatie vindt plaats door diverse authenticatiediensten van UWV zoals een Active Directory.
- Client / Server bedrijfsapplicaties (inclusief applicaties die een specifieke browser-plugin vereisen) zullen initieel via een virtuele werkplek (Citrix) benaderbaar blijven. UWV streeft echter naar steeds meer directe ontsluiting op het UWV-werkplek-device. Dit vereist dat dit device een beveiligde koppeling (VPN of meer fijnmazige oplossing) heeft met het datacenter van UWV voor de applicaties waarvoor de gebruiker geautoriseerd is. Voor de werkplekleverancier (kavel Werkplekdiensten) dient het mogelijk te zijn om de client-software op de werkplek-devices te kunnen installeren en updaten.

Om inzage te geven in bovengenoemde types applicaties, en het beschikbaar stellen hiervan op het UWV-werkplek-device, is onderstaande Tabel 4 opgenomen (indicatieve aantallen).

Type applicatie	Aantal
Microsoft 365 applicaties en moderne standaard applicaties (native apps)	50 +
Webbased SaaS-applicaties	40 +
Webbased on-premise hosted applicaties	200 +
Client/server on-premise hosted applicaties	90 +

Tabel 4: Overzicht en aantallen van type applicaties

De Netwerkdiensten zorgen voor veilige beschikbaarstelling van applicaties op basis van het zero-trust-principe. Dit betekent dat applicaties en services pas toegankelijk zijn, en (indien mogelijk) zichtbaar zijn op het netwerk, nadat de gebruiker (de identity) en het device geverifieerd zijn:

- Op basis van sterke authenticatie;
- En least-privilige-autorisaties het recht geven de applicatie of service te gebruiken;
- En continue de status van het verkeer en het gebruikte device gecontroleerd wordt en gecontroleerd kan worden op afwijkend gedrag en afwijkende gebeurtenissen (zoals in tijdstip, geolocatie, transacties);
- Ongeacht of de gebruiker op kantoor, thuis of onderweg werkt.

De moderne UWV-werkplek die altijd en overal kan worden gebruikt, is een kwetsbaar element in de ICT-keten. Het device wordt weliswaar continue geüpdatet en gemonitord maar is een high-risk-target en kent per definitie geen basaal vertrouwensniveau. Dit vertrouwen moet elke keer opnieuw gewonnen worden.

Voor gebruik van public cloud-diensten en SaaS applicaties, waarbij de web-gateway-functie geen efficiënte of goed werkende toegang kan bieden, ondersteunen de Netwerkdiensten een broker functie voor beveiligde toegang tot de betreffende diensten. Dit op basis van het bovengenoemde zero-trust-principe.
Voor toegang tot Microsoft 365 zal de Opdrachtnemer, in overleg met UWV en de werkplekdienstenleverancier (kavel Werkplekdiensten), de juiste rolverdeling moeten inrichten. De Microsoft 365 E5 tenant van UWV dient uiteraard goed beveiligd te zijn.

Voor ontsluiting van on-premises UWV-webapplicaties is een webapplicatie proxy wellicht een oplossing. Voor ontsluiting van UWV-client-server-applicaties op de moderne UWV-werkplek. ligt het voor de hand initieel een VPN-oplossing te gebruiken. UWV verwacht echter dat een (toekomstige) meer fijnmazige, moderne micro-VPN benodigd is. De oplossing dient te voorkomen dat ongeautoriseerd / niet-vertrouwd netwerkverkeer naar de bedrijfsapplicaties en datacenters van UWV mogelijk is. Tevens dient de oplossing te zorgen voor de afscherming en encryptie van data-in-transit. De geboden oplossing kan eventueel integreren en/of aansluiten op functies zoals het DXC-datacenter met VMware NSX-T segmentatie, of een Azure applicatie-proxy die in de UWV-Azure tenant gerealiseerd kan worden. Te denken valt ook aan de inzet van beschikbare oplossingen bij aangesloten datacenters. De meer specifieke keuzes die hier gemaakt kunnen worden, zullen in de UtI nader worden uitgewerkt. Dit geldt tevens voor de externe toegang voor gebruikers en beheerders van derde partijen.
De voor de veilige netwerkconnectiviteit benodigde instellingen op het UWV-werkplek-device worden bij voorkeur op basis van selfservice-onboarding gerealiseerd. De netwerkleverancier kan ook in samenwerking met de werkplekleverancier (delen van) deze benodigde inrichting realiseren. Daar waar encryptiesleutels en authenticatiesleutels gebruikt worden, voorzien de Netwerkdiensten in het (zoveel als mogelijk geautomatiseerd) beheer van de sleutels. De gehanteerde cyphersuites dienen ten minste te voldoen aan de richtlijnen van het NCSC.

5) Anti-(D)DOS-functie:
Werking en beschikbaarheid van de Netwerkdiensten mogen niet aangetast worden door (D)DOS aanvallen. Daarom dienen de delen van de Netwerkdiensten die aan het internet zijn gekoppeld beschermd te worden tegen (D)DOS en andere cybersecurity aanvallen.

6) Beveiliging van mailrelay en externe DNS:
De Netwerkdiensten dient beveiligingsmaatregelen voor mailrelay en externe DNS te bieden. Deze maatregelen zijn tenminste ingericht conform de Pas-toe-of-leg-uit overheidsrichtlijnen. Het betreft richtlijnen zoals STARTTLS, SPF, DKIM, DMARC, DNSSEC en DANE. De instellingen zullen getoetst worden (bijvoorbeeld via www.internet.nl en/of www.ssllabs.com). en zijn gericht op de bescherming van UWV-mail (en gebruikte domeinen in het DNS) tegen misbruik en inbreuk. De DMARC rapportages en logging zijn inzichtelijk voor UWV via een DMARC dashboard. Aanvullend geldt dat vanwege toegankelijkheid, beide diensten op basis van zowel IPv4 en IPv6 bereikbaar dienen te zijn. Daarnaast kan de inzet van DNS over HTTPS (DOH) overwogen worden.
De realisatie en bewaking van de samenhang tussen de beveiligingsinstellingen op de mailrelay-dienst en externe DNS-dienst zijn integraal onderdeel van de scope van deze aanbesteding. Aanpassingen vanwege toekomstige ontwikkelingen van richtlijnen behoren daarnaast ook tot de scope.
Gekoppelde email-omgevingen zijn:

- Microsoft 365 Outlook Online;
- Suwimail (op SUWINET);
- Belastingdienst;
- Een aantal SMTP agents van bedrijfsapplicaties.

Gebruik van de mailrelay-functie door de gekoppelde email-omgevingen wordt toegestaan op basis van whitelisting. De mailrelay-dienst heeft naast de routeringsfunctie, ook een uitgebreide inspectie en schoningsfunctie. Deze functies zorgen ervoor dat ontvangen en verzonden mails geen virussen of andere malicious content bevatten en SPAM effectief verwijderd wordt. De inspectie dient te geschieden op basis van altijd actuele algoritmes en dreigingsinformatie.

Een deel van de mailrelay functie kan in de toekomst onderdeel gaan uitmaken van de Microsoft 365 omgeving van UWV. Mogelijk zal de netwerkleverancier een beheerrol gaan invullen voor het beheer van de aldaar benodigde beveiligingsinstellingen. Verdere invulling van deze dienst volgt in de UtI-fase.

7) Beveiligd VoIP koppelvlak:
Op het scheidsvlak tussen de UWV-kantoornetwerken en diensten voor telefonie en Contactcenter bieden de Netwerkdiensten een beveiligd VoIP-koppelvlak. Dit beveiligd koppelvlak vormt het demarcatiepunt tussen telefonie en Contactcenter gerelateerd VoIP/SIP verkeer en het WAN/LAN van UWV. Te denken valt aan Session Border Controller functionaliteit. Het VoIP koppelvlak biedt ondersteuning voor het aansluiten van SIP-trunks van de telefonie- en Contactcenter diensten leverancier. VoIP-devices in kantoren van UWV kunnen hierdoor op beide diensten worden aangesloten, eventueel op basis van SIPS en SRTP.
UWV verwacht overigens dat met name de Contactcenter diensten in de toekomst gebruik zal gaan maken van (secure) WebRTC technologie, maar dit geldt mogelijk ook voor andere VoIP diensten.

8) Integratie, policies, en actualiteit van de Netwerkdiensten:
Opdrachtnemer levert een zo veel als mogelijk geïntegreerde netwerk- en securitydiensten op basis van centrale besturing en centraal policybeheer. Deze integratie draagt bij aan de kwaliteit van het end-to-end beveiligingsniveau en de netwerkprestaties. Daarnaast wordt end-to-end-performance en security-monitoring eenvoudiger en wordt het beheer van security-policies en netwerkinstellingen overzichtelijker en effectiever. Gehanteerde policies, algoritmes, dreigingsinformatie en signatures voor preventie, inspectie en mitigatie dienen altijd actueel, compliant, en beschikbaar te zijn. De UWV-ICT-infrastructuur, de UWV-werkplek-devices en overige aangesloten diensten en devices dienen te worden ondersteund met een zo hoog mogelijk beschermingsniveau van de Netwerkdiensten. Hierbij faciliteren en adopteren de Netwerkdiensten beproefde ontwikkelingen en updates van dienstonderdelen, zijnde vernieuwingen die bijdragen aan een hoger beschermingsniveau. De inzet van Artificial Intelligence voor meer geavanceerde analyse en anomaly detection is hier een voorbeeld van. UWV verwacht inzake actualiteit en vernieuwing dan ook een Evergreen-benadering.

9) Mogelijke integratie met Enterprise Mobility Management (EMM)
UWV overweegt de Netwerkdiensten functionaliteit ook voor gecontroleerde applicatieontsluiting naar de smartphones (managed/unmanaged) in te zetten. Dit is afhankelijk van de ontwikkelingen binnen de Werkplekdiensten en de Telefoniedienst van UWV. In de UtI fase zal dit onderwerp nader worden toegelicht.

4.6 *Beheerdiensten*

Voor de regievoering op operationeel, tactisch en strategisch niveau zal de leverancier van de Netwerkdiensten participeren in een vooraf afgesproken governance structuur. De aan UWV geleverde Netwerkdiensten zijn zo veel als mogelijk uitbestede en integraal beheerde diensten. De dienstverlening is ingericht op basis van duidelijk gedefinieerde ITIL-koppelvlakken met UWV. De beheerdiensten die ten minste onderdeel uitmaken van de scope van deze aanbesteding zijn:

- Opdrachtnemer is verantwoordelijk voor de beschikbaarheid, continuïteit en vereiste werking van de netwerk- en securityfuncties en onderliggende infrastructuur. Opdrachtnemer levert de dienst en beheerdienstverlening conform afgesproken servicelevels. De Opdrachtnemer houdt vanuit die rol operationeel toezicht middels security- en infrastructuurmonitoring;
- De Netwerkdiensten worden geleverd inclusief life cycle management. Hieronder wordt verstaan het actueel en onder support houden van software, hardware en instellingen van de Netwerkdiensten. Opdrachtnemer rapporteert om die reden periodiek over de hardware en software assets incl. softwareniveaus en patches. Ongeacht of dit een shared service betreft;
- Opdrachtnemer levert de integratorrol voor netwerkkoppelingen met andere ICT-diensten (zowel on-premises als cloud-diensten), ketenpartners en UWV. De Opdrachtnemer werkt om die reden samen met meerdere leveranciers die verantwoordelijk zijn voor andere (ICT-)kavels.

De Opdrachtnemer draagt zorgt dat de functionaliteiten werken conform de behoeftestelling van UWV. Eventueel kan de Opdrachtnemer aan UWV adviseren het bedienen van de Netwerkdiensten (bijvoorbeeld selfservice op het vlak van standaard changes van functionele instellingen) op onderdelen bij UWV te beleggen. Zolang dit kostenbesparend is, bijdraagt aan de flexibiliteit en verandersnelheid en geen operationele risico’s introduceert.
In de volgende paragrafen volgt een nadere toelichting van een aantal beheerdiensten.

4.6.1 Servicedesk, ITSM en monitoring

Net zoals in de huidige situatie behoudt UWV een eerstelijns servicedesk waar alle servicecalls gemeld worden. Deze servicedesk is open op Werkdagen van 07.00 tot 19.00 uur. Buiten die tijden is er bij UWV een telefonisch escalatiepunt, voor het melden en afhandelen van grote incidenten.
De Opdrachtnemer voor Netwerkdiensten biedt een tweedelijns servicedesk en derdelijns support naar betrokken leveranciers en productvendoren. UWV stuurt de Opdrachtnemer op incidenten die uit de tijd dreigen te lopen, en/of op kaveloverstijgende incidenten. De ITSM-tooling van de Opdrachtnemer dient gekoppeld te worden met de ITSM-tool van UWV. Hiermee wordt automatische uitwisseling van servicecalls en CMDB onderdelen mogelijk, ter ondersteuning van de operationele processen.
De netwerkleverancier bewaakt de end-to-end functionele werking op kwaliteit, capaciteit en beschikbaarheid. Mogelijke afwijkingen worden opgevolgd zodanig dat levering conform SLA geborgd is. De Opdrachtnemer biedt UWV middels online dashboards inzicht in de status van de diverse dienstonderdelen op relevante aspecten zoals topologie, capaciteit en verbruik, performance en beschikbaarheid, beveiliging en binnen de dienstonderdelen gehanteerde instellingen en policies.
Beschikbaarheid van bedrijfsprocesketens is voor UWV van vitaal belang. Om dit mogelijk te maken heeft UWV een UWV Monitoring Operations Center (UMOC) ingericht. Hiermee heeft de regieorganisatie van UWV inzicht in de beschikbaarheid en performance van bedrijfsketens en onderliggende applicaties en infrastructuur. Voor de door het UMOC

gebruikte bedrijfsapplicatie-ketenmonitoring, zorgt de Opdrachtnemer voor de aanlevering van relevante events en logs vanuit diverse netwerkonderdelen. Waar nodig worden agents ingezet.

4.6.2 Security, risk en compliance management

De Opdrachtnemer biedt security beheer- en security monitoringfunctie (bijvoorbeeld een SOC). Hieruit worden continu alle beveiligingsmaatregelen binnen de scope en op de grensvlakken van de dienstverlening gemonitord. Deze functie correleert de status en de signalen (logging en events) afkomstig van deze beveiligingsmaatregelen en neemt bij afwijkingen actie om het beveiligingsniveau te herstellen. De Opdrachtnemer verstrekt relevante logdata en events aan het door het USOC gebruikte SOC/SIEM systeem, waarmee het USOC de beveiliging van de gehele ICT-keten van UWV bewaakt. De Netwerkdiensten bieden UWV realtime inzage in de werking van het gehele pakket aan beveiligingsmaatregelen en geconstateerde afwijkingen. Hiervoor worden relevante dashboards geboden.
De Opdrachtnemer geeft daarnaast invulling aan risk management, met onder andere risk inventarisatie, -registratie en -analyse, risk mitigatie plannen en -implementatie, en het uitvoeren van audits.
De Opdrachtnemer bewaakt de compliance en biedt inzicht in de compliance status van de Netwerkdiensten. Dit kan bijvoorbeeld door middel van certificeringen, assurance verklaringen, aangevuld met GRC-dashboards (continuous compliance).

4.6.3 BKN-beheer

In alle gebouwen van UWV ligt een gecertificeerd horizontaal- en verticaal bedrijfskabelnetwerk (BKN) waarvan UWV de eigenaar is en blijft. Door het ‘WiFi tenzij’-principe zal de UWV-gebruiker op kantoor veelal het Wireless LAN gebruiken. Dit heeft tot gevolg dat het gebruik van bedrade LAN-verbindingen en LAN-switch-poorten zal gaan afnemen ten opzichte van de huidige situatie. Het aantal mutaties zal derhalve veel minder groot zijn dan de afgelopen jaren het geval was. De Opdrachtnemer voorziet in het beheer van het BKN (horizontaal, verticaal, patchkasten, patchkabels, aansluitkabels en patchpanelen). De BKN-beheerdienst is voornamelijk gericht op de koppelingen tussen (Wireless)LAN-apparatuur en het beschikbaar stellen van LAN op outlets op de verdiepingen. De Opdrachtnemer voorziet daarnaast in onsite IMACD dienstverlening van patchmutaties (BKN, LAN, outlet) aangevraagd door UWV. De mutaties dienen te worden bijgehouden in een patch-management-administratie. Tot slot voorziet de Opdrachtnemer in projectmatige levering, aanleg, verwijdering van een BKN bij herindeling van panden, grootschalige verhuizingen of inrichting van nieuwe panden. Deze werkzaamheden kunnen worden gecombineerd met de aanleg van (Wireless)LAN en/of WAN op de kantoren. Naar verwachting zal het aantal grootschalige verhuizingen of inrichting van nieuwe panden beperkt zijn tot enkele projecten per jaar.

4.6.4 MER en SER beheer

Elk kantoor kent een aantal technische ruimtes. Deze Main Equipment Rooms (MER’s) en Satellite Equipment Rooms (SER’s) beschikken over klimaat-, brandblus- en noodstroomvoorzieningen. Tevens staan er in diverse kantoren High Availability Cabinets (HAC’s) met ingebouwde soortgelijke omgevingsbeheervoorzieningen. Deze HAC’s zijn beveiligd met toegangsbewaking op afstand. UWV is en blijft eigenaar van alle voorzieningen en kasten in de technische ruimtes. Door de opkomst van de Microsoft 365 werkplek en het ‘WiFi tenzij’ principe zal het aantal servers en switches in de MER’s en SER’s gaan afnemen. Voor software updates op de UWV werkplek devices worden nu nog in de meeste kantoren caching servers ingezet. In de nieuwe situatie worden de Microsoft Intune-managed

werkplekken rechtstreeks geüpdate via internet. Door de afname van ICT-apparatuur zullen de benodigde MER- en SER-voorzieningen daarom in omvang en capaciteit afnemen. De Opdrachtnemer voorziet binnen de scope van de opdracht in een beheer- en onderhoudsdienst van de in de MER's en SER's aanwezige apparatuur voor noodstroom-, klimaat- en brandblusvoorzieningen. De netwerkleverancier houdt daartoe een onderhoudsschema en CMDB bij zodat apparatuur tijdig vervangen wordt. Bij deze vervanging zal bekeken worden of apparatuur nog noodzakelijk is, gezien de verwachte afname van ICT apparatuur in MER's en SER's. Tevens coördineert de Opdrachtnemer de vervanging in samenwerking met de door facilitair bedrijf van UWV gecontracteerde leveranciers. Tot slot bewaakt de netwerkleverancier op afstand de toegang tot de HAC's, zodat alleen bevoegd personeel toegang heeft.

4.6.5 Integratie-, ontwerp-, en adviesdienst

De ICT-infrastructuur van UWV verandert als gevolg van nieuwe diensten, vernieuwing van bestaande diensten en transities voortvloeiend uit aanbestedingen. De Opdrachtnemer biedt een architectuurfunctie voor netwerk en security voor de juiste integratie van alle ICT-onderdelen en wijzigingen. Tevens levert de Opdrachtnemer design-, bouw- en projectcapaciteit voor de grote veranderprojecten.
UWV vraagt periodieke gevraagde en ongevraagde (proactieve) advisering en voorstellen voor innovatie, vernieuwing, milieuvriendelijke levering en life cycle management. Deze adviezen worden door Opdrachtnemer verwerkt in afgestemde roadmaps. Dit stelt UWV tijdig in staat om, samen met de netwerkleverancier en overige ICT-leveranciers, de projecten, budgetten en resources in te plannen. Opdrachtnemer is bijvoorbeeld sturend in het begeleiden en realiseren van op zero-trust gebaseerde Netwerkdiensten bij UWV. Deze verandering strekt zich over de volle breedte van de UWV-infrastructuur uit.
De Opdrachtnemer biedt de benodigde periodieke opleiding en instructies aan UWV-medewerkers. Dit bijvoorbeeld ten behoeve van het gebruik van dashboards en het eventueel op onderdelen uit te voeren functioneel beheer (selfservice) van de netwerk- en security-instellingen.

4.7 *Koppelvlakken*

UWV heeft in de toekomst diverse externe koppelvlakken inzichtelijk en in beheer. Deze koppelvlakken zijn op hoofdlijnen onder te verdelen in de onderstaande categorieën:

1. Externe koppelingen: Dit betreffen integraties met systemen van ketenpartners van UWV, ten behoeve van applicatietoegang en informatie uitwisseling;
2. Internet gebaseerde koppelingen: Dit betreffen koppelingen met cloud based diensten en internettoegang (voor werkplek, Microsoft 365, KPN HotSpot en het applicatiedatacenter van DXC);
3. Datacenter-koppelingen: Dit betreffen aansluitingen van/ functionele koppelvlakken met datacenters voor de werkplek, hosting van bedrijfsapplicaties, telefonie, printing, Contactcenter diensten en gebouwbeveiliging.

Onderstaande Tabel 5 beschrijft de belangrijkste toekomstige functionele koppelvlakken in meer detail:

Nr.	Kavel/Dienst/Thema	Toelichting
1	Werkplekdiensten – Microsoft 365 Werkplekken UWV	Veilige en efficiënte netwerkkoppeling van de Moderne Werkplek, zodat Anywhere toegang mogelijk is naar alle gebruikte toepassingen.

Nr.	Kavel/Dienst/Thema	Toelichting
2	Werkplekdiensten Werkplekken UWV – Datacenter koppeling	Koppeling met KPN-werkplekdatacenters, ten behoeve van toegang vanuit kantoren UWV tot de "oude" werkplekdienst van KPN Werkplek. Deze werkplekdienst is volledig gebaseerd op een virtuele werkplek. De dienst wordt vanaf 2022 langzaam maar zeker afgebouwd. Niet zeker is wanneer deze dienst beëindigd wordt.
3	Werkplekdiensten Active Directory – Datacenter koppeling en externe koppeling	Koppeling met de on-premises Active Directory en/of Azure Active Directory voor authenticatie- en autorisatiedoeleinden.
4	Telefonie (Externe koppeling)	In de loop van 2022 zal naar verwachting een nieuwe telefonieleverancier worden aangesloten. Het technisch (SIP) koppelvlak blijft gelijk. De telefoniefuncties zullen vanuit een hosted voice oplossing van de opvolgend telefonieleverancier geleverd worden. In het netwerk van UWV blijven VoIP soft- en hardphones gebruikt worden.
5	Huidige Contactcenter diensten – Datacenter koppeling	Beveiligd koppelvlak tussen UWV en de Contactcenter diensten, geleverd vanuit twee datacenters van Capgemini. Het netwerk van UWV wordt via een redundant WAN-koppelvlak aangesloten op deze dienst, ten behoeve van data en VoIP-verkeer. Het VoIP-verkeer wordt ontsloten via het beveiligd VoIP-koppelvlak (welke ook voor de telefoniedienst gebruikt wordt).
6	Toekomstige Contactcenter diensten – nog nader te bepalen	Beveiligd koppelvlak tussen UWV en de in 2024/2025 verworven Contactcenter diensten, voor applicatief en voice verkeer. Naar verwachting zal WebRTC zijn intrede doen.
7	Bedrijfsapplicatie DC Kyndryl t.b.v. interne bedrijfsapplicaties	Een redundant WAN met de datacenterdienst van Kyndryl. Gedurende 2022 en 2023 worden applicaties gemigreerd naar de DXC-datacenters. Naar verwachting zal rond eind 2023 dit koppelvlak uitgefaseerd zijn.
8	Bedrijfsapplicatie DC DXC t.b.v. interne bedrijfsapplicaties	Een redundant WAN met de Datacenterdienst van DXC. In de loop van 2023 zullen de E-diensten via een nieuw beveiligd internetkoppelvlak, inclusief reverse proxy en web application firewall functie, bij DXC aangesloten gaan worden. De migratie van alle bedrijfsapplicaties naar het DXC-datacenter zal naar verwachting tot eind 2023 duren.
9	Dienst Multifunctioneel afdrukken – Datacenter koppeling	Koppelingen tussen Xerox-printerfunctionaliteit op bedraad LAN en de centrale Xerox-printerservers gehost bij KPN. Na 2024 zal dit koppelvlak mogelijk migreren naar een andere leverancier en andere technologie.

Nr.	Kavel/Dienst/Thema	Toelichting
10	Derde partijen en (overheids)partners – Externe koppelingen	Beveiligde WAN-, VPN- en DCI-verbindingen met diverse instanties en derde partijen. Deze verbindingen worden gebruikt voor data-uitwisseling met die derde partijen, voor beheeractvitiviteiten door derde partijen, en voor toegang tot werkplekfuncties en bedrijfsapplicaties vanuit ketenpartners (SUWI).
11	Internet (filtered) – internet koppeling	Beveiligde koppelingen met het internet ten behoeve van browse verkeer van de UWV-werkplek en voor diverse multimedia-diensten zoals newsroom en studio's.
12	Internet (open) – internet koppeling	Beveiligde koppelingen met het internet ten behoeve van browse verkeer van bezoekers en govroam gebruikers.
13	SOC/SIEM dienst UWV – via datacenter koppeling	Beveiligd koppelvlak met de SOC/SIEM oplossing van UWV bij DXC, voor beschikbaar stellen van security logging en gebruikersmonitoring.
14	Gebouwbeveiliging – Datacenter koppeling	Koppelen van gebouwbeveiligings-devices op bedraad LAN met het datacenter van de dienst gebouwbeveiliging in het datacenter van KPN.
15	Performance & Beschikbaarheidsmonitoring – via een Datacenter koppeling	Beveiligd koppelvlak voor beschikbaar stellen van event-data van diverse netwerkonderdelen aan de UWV centrale dienst Bedrijfsapplicatieketenmonitoring.
16	ITSM-Tooling – internet koppeling	Omnitracker is UWV's ITSM-platform waarmee servicecall integratie met de ITSM van de Opdrachtnemer plaatsvindt.

Tabel 5: Toekomstige functionele koppelvlakken van de Netwerkdiensten

4.8 *Transitie, transformatie en re-transitie (exit)*

Om de toekomstige situatie van Netwerkdiensten te bereiken, voorziet UWV dat een transitie en transformatie moeten plaatsvinden. Deze periode zal naar de inschatting van UWV circa 16 maanden duren. De scope van de opdracht van deze aanbesteding dient gedurende deze periode bedrijfsklaar en turn-key te worden opgeleverd. Het transitie- en transformatieproject vangt (direct) aan na ondertekening van het contract en begint met een periode van voorbereiding.

Het transitie- en transformatieproject bestaat uit de implementatie en configuratie van Netwerkdiensten. Onderdeel is onder andere de migratie van de UWV-kantoren van de huidige situatie van de netwerkoplossing naar de toekomstige situatie. Conform een nader te bepalen volgorde en aanpak wordt het transitie- en transformatieproject gefaseerd en gecontroleerd uitgevoerd. Indien er deelopleveringen plaatsvinden, zal voor die deelopleveringen de dienstverlening al conform overeenkomst en gemaakte afspraken plaatsvinden. In de UtI zullen uitgangspunten ten aanzien van het transitie- en transformatieproject zijn opgenomen. Uiteraard dient rekening te worden gehouden met re-transitie (exit) afspraken met de huidige leverancier (KPN). Tijdens het transitie- en transformatieproject zijn de continuïteit van de koppelvlakken van uiterste belang. Een aantal koppelvlakken zullen tijdens het transitie- en transformatieproject nog kunnen

veranderen door transitie- en transformatieprojecten van andere ICT-kavels (bijvoorbeeld het kavel Werkplekdiensten). Na de transitie en transformatie van de Netwerkdiensten vindt decharge van het project plaats, waarna de uitvoering van de overeenkomst conform de gemaakte afspraken dient plaats te vinden.

Gedurende de uitvoering van de overeenkomst gaat afhankelijk van ontwikkelingen zoals innovaties een verdere transformatie plaatsvinden. De Opdrachtnemer draagt zorg voor het actueel en technologisch op niveau houden van de Netwerkdiensten aansluitend op de functionele eisen, architectuurkaders en het cloud- en securitybeleid van UWV.

In het geval van een (tussentijdse) beëindiging van de Overeenkomst na de initiële looptijd of (tussentijdse) beëindiging na een verlenging wordt de verantwoordelijkheid voor de dienstverlening (geheel of gedeeltelijk) overgedragen. Overdracht vindt in dit geval plaats op basis van een actueel en toepasbaar re-transitieplan van de Opdrachtnemer naar een nieuwe verkrijgende leverancier of UWV. De diensten die behoren bij een re-transitie maken onderdeel uit van de scope van deze aanbesteding.

4.9 *Diensten optioneel in scope*

Er worden geen optionele diensten uitgevraagd.

4.10 *Diensten niet in scope*

Onderstaande oplossingen en diensten maken nu deel uit van het KPN-contract maar maken geen onderdeel uit van de scope van de opdracht:

- Internet koppelvlak DXC datacenter voor ondermeer E-diensten – omvattende Internetlijn, WAF, reverse proxy, forward proxy - gaat naar het DXC-contract;
- Bedrijfsapplicatieketenmonitoring. UWV overweegt deze dienst als een separate dienst aan te besteden dan wel op andere wijze in te vullen;
- PKIoverheid – Voor de machine-to-machine koppelingen. UWV zal deze dienstverlening separaat contracteren;
- eHerkenning: Betreft een specialiteit die niet tot de core van Netwerkdiensten behoort. Het betreft een dienst voor de applicaties van UWV die gericht zijn op de klanten van UWV. UWV zal deze dienst separaat contracteren;
- CDN (Content Delivery Network)– Betreft een specialisme voor het ondersteunen van webcontent en videocontent. UWV zal deze dienst separaat contracteren.

5. Definities

In deze bijlage hebben de woorden die met een hoofdletter worden geschreven, zowel in enkelvoud als in meervoud, de navolgende betekenis. Voor begrippen die niet in deze lijst zijn vermeld verwijzen wij naar de definities opgenomen in hoofdstuk 1 van het document Uitnodiging tot Aanmelding Netwerkdiensten 2022.499.

Begrip	Definitie
Anywhere	Thuis, onderweg en op kantoor.
Azure Active Directory	De identiteits- en toegangsbeheerservice in de cloud van Microsoft, waarmee medewerkers zich kunnen aanmelden en toegang kunnen krijgen tot resources.
Bedrijfsapplicatieketen-monitoring	End-to-end monitoringdienst van bedrijfskritische applicaties door middel van het monitoren van de applicatieketen en de onderliggende infrastructuur.
BIO	De Baseline informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen).
BIR	De Baseline Informatiebeveiliging Rijksdienst (BIR) is een specifieke invulling van de ISO 27002 norm voor de beveiliging van informatie(systemen) van de Rijksdienst.
BIV	Een BIV-classificatie of BIV-indeling is een indeling die binnen de informatiebeveiliging wordt gehanteerd, waarbij de beschikbaarheid, de integriteit en de vertrouwelijkheid van informatie en systemen wordt aangegeven. BIV is het acroniem voor Beschikbaarheid, Integriteit, Vertrouwelijkheid.
CMDB	Configuration Management Database is een database voor configuratiebeheer en is een ITIL-term voor een database die door een organisatie wordt gebruikt om informatie over hardware- en software activa op te slaan.
Contactcenter diensten (CCD)	Diensten ingericht bij UWV voor het afhandelen van telefoongesprekken, chat- en e-mailberichten.
DANE	DNS-based Authentication of Named Entities is een protocol voor het veilig publiceren van publieke sleutels en certificaten.
DKIM	DomainKeys Identified Mail is een techniek waarbij een organisatie verantwoordelijkheid kan nemen voor een bericht dat per e-mail wordt verzonden.
DMARC	Domain-based Message Authentication, Reporting and Conformance is een verificatie protocol voor e-mail om e-maildomeinen te beschermen tegen ongeoorloofd gebruik.
Drivers of Change	Ontwikkelingen die de toekomstige inrichting van Netwerkdiensten beïnvloeden en zal doen veranderen.
E-diensten	Betreft de volledige voorziening van digitale dienstverlening aan UWV klanten.
Edge	Scheidingsvlak tussen het lokale netwerk en het koppelvlak richting het internet.
eHerkenning	Gestandaardiseerd inlogsysteem waarmee organisaties hun diensten veilig online toegankelijk kunnen maken.

Begrip	Definitie
Evergreen-benadering	Benadering waarbij alle diensten te alle tijden gemanaged worden in die mate dat deze up-to-date wordt gehouden en voldoet aan de noodzakelijke richtlijnen en voorschriften.
Forum Standaardisatie	Een adviescommissie met deskundigen uit diverse overheidsorganisaties, het bedrijfsleven en de wetenschap.
govroam	Onafhankelijk netwerkservice provider voor overheidsinstellingen die overheidsorganisaties in staat stelt netwerken met elkaar te delen.
GRC	Proces dat ondersteuning biedt aan het inrichten en handhaven van een set aan normen en wetten gebaseerd op Governance, Risicobeheer en Compliance.
ISO 27001	Is een ISO standaard voor informatiebeveiliging die tevens wereldwijd erkend is als norm op het gebied van informatiebeveiliging.
ITIL	Information Technology Infrastructure Library ontwikkeld als een referentiekader voor het inrichten van beheerprocessen binnen de ICT-organisatie.
IV-infrastructuur	De onderliggende infrastructuur die de Informatievoorziening van UWV, de geautomatiseerde informatiesystemen en de niet-geautomatiseerde informatie-items die gebruikt worden, ondersteunt.
IV-middelen	Alle ICT-middelen en diensten ter ondersteuning van één of meerdere bedrijfsprocessen.
Keten Regie Loket	UWV organisatie verantwoordelijk voor dagelijkse monitoring van bedrijfsapplicaties en de onderliggende infrastructuur. Hiernaast bij geconstateerde afwijkingen coördinerend bij escalaties.
Koppelvlakken	Netwerkkoppelpunten om een gecontroleerde doorgang mogelijk te maken van het ene netwerk naar het andere.
KPN HotSpot	KPN dienst die faciliteert in het aanbieden van draadloos internet voor bezoekers via WiFi.
KPN ONE	KPN dienst die een zakelijke oplossing biedt op het gebied van bedrijfscommunicatie.
KPN-Werkplek(diensten)	Zakelijke oplossing van KPN die alle UWV medewerkers voorziet van een virtuele werkplek inclusief de aanverwante technische inrichting.
KWN	Kantoorautomatisering, Werkplek- en Netwerkdiensten.
KWN-diensten	Betreft alle diensten die KPN aan UWV levert vanuit het overkoepelende KWN-contract.
KWNTC	Kantoorautomatisering, Werkplekmiddelen, Netwerk, Telefonie en Contactcenter diensten.
Microsoft 365	Een verzameling van Microsofts internetdiensten, veelal aangeboden als online dienst.
Microsoft Teams	Communicatie- en samenwerkingsplatform van Microsoft.
Moderne Werkplek	Microsoft Windows gebaseerde werkplek device, voorzien van Microsoft 365 software.
NCSC	Het Nationaal Cyber Security Centrum is een publiek-private Nederlandse organisatie die de weerbaarheid van de Nederlandse samenleving in het digitale domein tracht te vergroten.

Begrip	Definitie
Netwerkbeveiliging	Richt zich op het treffen van maatregelen om de risico's ten aanzien van de communicatie via netwerken te controleren en beheersen.
Netwerkdiensten	Betreft alle diensten in scope die onderdeel uitmaken van de aanbesteding UWV Netwerkdiensten.
NL-IX	Internetknooppunt / peering-netwerk in Nederland.
OWASP	Open Web Application Security Project is een non-profitorganisatie die zich inzet voor het verbeteren van computerbeveiliging. Dit doen ze o.a. door het uitbrengen van adviezen en rapportages
Pas toe of leg uit	Beleid voorgeschreven door Forum Standaardisatie die overheidsorganisaties verplicht stelt standaarden toe te passen.
PKIoverheid	De Public Key Infrastructure van de Nederlandse overheid.
SMW	Betreft het UWV ICT programma 'Samen naar de Moderne Werkplek' waaronder meerdere projecten zijn gedefinieerd.
Suwinet	Digitale infrastructuur die ontwikkeld is om ervoor te zorgen dat de SUWI-partijen (UWV, SVB en gemeenten) gegevens met elkaar kunnen uitwisselen voor de uitoefening van hun wettelijke taak.
SUWI-wet	Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI-wet).
UWV-Koppeldienst (UKD)	Betreft de centrale beveiligingsinfrastructuur bestaande uit diverse beveiligingscomponenten en geldt als centraal koppelpunt voor alle kantoren, ICT-diensten en externe netwerken.
Verkeerscategorieën	Indeling van verkeersstromen in categorieën op basis van type verkeer en technische eigenschappen.
Verkeersstromen	Het differentiëren van over het netwerk getransporteerd dataverkeer, op basis van karakter en technische eigenschappen.
Werkplekdiensten	Alle diensten in scope die onderdeel uitmaken van de aanbesteding Werkplekdiensten.
Werkplekmiddelen	Omvat de hardware en het beheer van de apparatuur op de werkplek en alle op kantoor noodzakelijke diensten ter ondersteuning van de apparatuur.
Zero-trust	Het zero trust-beveiligingsmodel ('perimeterless security') beschrijft een benadering van het ontwerp en de implementatie van IT-systemen waarbij per definitie de identiteit van de gebruiker en/of het device niet vertrouwd is.