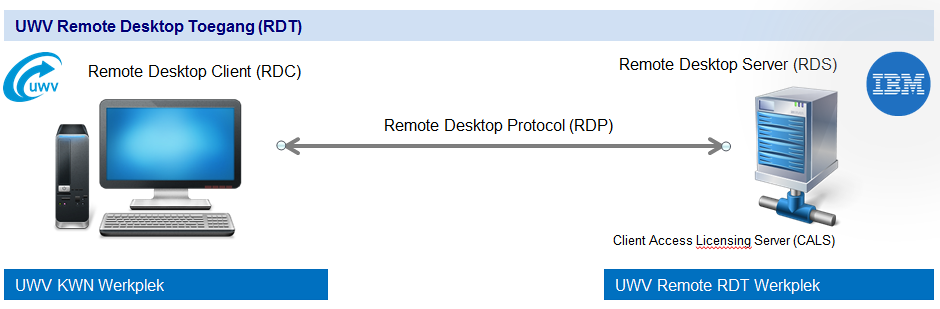
|  |  |
| --- | --- |
|  | **2016** |
|  | UWV  Berg, Rene van den (R.) |

|  |
| --- |
| **[**RemoteDesktopToegang**]** |
| Extract uit het OTAP beleid en context beschrijving voor Remote Desktop Toegang (RDT) |



Inhoud

[1. Inleiding en positionering 2](#_Toc440615051)

[1.1. Inleiding / doelstelling 2](#_Toc440615052)

[1.2. Uitgangspunten 2](#_Toc440615053)

[1.3. Afwijkingen via ‘Comply or Explain’ 2](#_Toc440615054)

[1.4. De zonering 2](#_Toc440615055)

[2. Beleid 3](#_Toc440615056)

[2.1. Relevante IV doelstellingen 3](#_Toc440615057)

[2.2. Afbakening RDT 4](#_Toc440615058)

[2.3. Positionering en inrichting RDT 4](#_Toc440615059)

[2.4. ICT Strategie & Beleid 6](#_Toc440615060)

[3. Uitvoeringsdomein 7](#_Toc440615061)

[3.1. Doelstelling 7](#_Toc440615062)

[3.2. Toegang 7](#_Toc440615063)

[3.3. Communicatie en koppelingen 9](#_Toc440615064)

[4. RDT bij UWV 11](#_Toc440615065)

[4.1. Context 11](#_Toc440615066)

[4.2. Huidige situatie 12](#_Toc440615067)

[4.3. Gewenste situatie 12](#_Toc440615068)

[5. Begrippen en definities 12](#_Toc440615069)

# Inleiding en positionering

## Inleiding / doelstelling

Deze notitie is een extract uit het OTAP beleid specifiek gericht op toegang via het Remote Desktop protocol (RDP). Het gebruik van toegang via RDP voor beheer doeleinden is in een ultieme situatie een onwenselijke voorziening. Het liefst zien we toegang tot de applicatie geregeld via applicatiefuncties waaraan gebruikers gekoppeld zijn. In de diversiteit van het UWV ICT landschap is het nodig gebleken om buiten de applicatie om toegang te verlenen, onder andere voor uitvoering van ontwikkel en test werkzaamheden. Daartoe is het Remote Desktop Toegang omgeving in het leven geroepen. In de loop der jaren zijn er vele nieuwe verschillende remote desktop servers in gebruik genomen waar eigenlijk een beperkt aantal zou volstaan. De huidige situatie kent o.a. een risico t.a.v. de toegangslogging en het Identity Management. Een centrale omgeving zou een groot deel van de beveiligingsproblematiek oplossen en tevens een kostenreductie betekenen.

In het vervolg van deze notitie worden vingerend beleid voor de dienst Remote desktop toegang richting het UWV HRC en de invulling hiervan toegelicht.

## Uitgangspunten

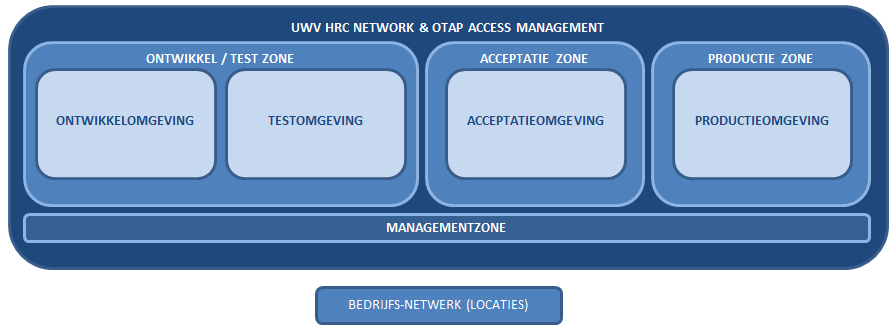
Ten aanzien van OTAP voorzieningen zijn de normen uit de UWV BIR (Baseline Informatiebeveiliging Rijksdienst) van toepassing. RDT maakt hier onderdeel vanuit. Deze BIR richtlijnen, aangevuld met specifiek voor UWV geldende beveiligingscriteria, zijn het uitgangspunt om te voldoen aan het door UWV vastgestelde Informatiebeveiligingsbeleid.

## Afwijkingen via ‘Comply or Explain’

De geldende (beleid)richtlijnen en architectuurprincipes zijn kader stellend. Bij de toepassing van deze richtlijnen en principes mag, mits gemotiveerd en in overeenstemming met de eigenaar van de richtlijnen en principes, daarvan worden afgeweken.

## De zonering

Een OTAP-zone garandeert de integriteit van de omgevingen en de gebruikte gegevens. Er kunnen meerdere zones van hetzelfde type, uitgezonderd de managementzone, in één rekencentrum voorkomen, zoals de productiezone van het Werkbedrijf naast de productiezone van UWV.



In het UWV HRC zijn vier zones te onderscheiden (logisch of fysiek gescheiden netwerksegmenten waartussen communicatie / verkeer alleen op een gecontroleerde manier kan / mag plaatsvinden). Dat zijn de ontwikkel/test zone (OT-zone), acceptatiezone (A-zone) en een productiezone (P-zone). Daarnaast biedt een managementzone (M-zone) ondersteuning op het gebied van de toegang tot de andere zones en het verkeer, transport van gegevens en software, tussen de verschillende omgevingen in de zones.

# Beleid

Dit hoofdstuk geeft een extract van de beleidsrichtlijnen die betrekking hebben op RDT.

## Relevante IV doelstellingen

De beleidsuitgangspunten voor OTAP zijn een direct afgeleide van de volgende IV Principes

|  |  |
| --- | --- |
| P3. Invulling van de IV op basis van in de markt of bij de overheid gangbare suites/ bouwblokken. | |
| Toelichting: | Bij het (her)invullen van (nieuwe) functionele wensen geldt de volgorde hergebruik, kopen, maken. Hierbij worden bij voorkeur overheid brede en/of op de markt verkrijgbare generieke bouwstenen gebruikt in de vorm van bewezen en toekomst vaste standaard­pakketten en frameworks, ook in combinatie met andere bouwstenen. Applicaties worden afgebakend op basis van relatieve autonomie (door binnen onderdelen te streven naar maximale samenhang en tussen onderdelen naar minimale afhankelijkheid), zelfstandig bestaansrecht en kleine functionele eenheden die projectmatig efficiënt gerealiseerd kunnen worden. Waar functioneel vergelijkbaar, moeten de applicaties afgebakend worden conform gangbare in de markt verkrijgbare equivalenten. Beproefde middelen worden verkregen vanuit een Best-of-suite benadering per aandachtsgebied.  In de UWV-informatievoorziening is er voor elke functionaliteit slechts één component operationeel. In het IV-landschap worden middelen ingezet die specifiek voor een functioneel gebied zijn ontwikkeld. |
| Rationale: | UWV heeft ICT nodig voor haar kerntaak. Het goedkoop en doelgericht kunnen inzetten van ICT is belangrijker dan het zelf ontwikkelen hiervan. Om afhankelijkheid van leveranciers te minimaliseren of om te voorkomen dat UWV wordt geconfronteerd met (grote) onvolkomenheden in de verkregen ICT worden strenge eisen gesteld aan (bewezen) kwaliteit en toekomstvastheid.  UWV houdt in haar ICT-landschap optimaal rekening met het kunnen inzetten van inzet van overheidsbouwblokken en middelen uit de markt. Afhankelijkheid van leveranciers wordt hiermee verminderd. Tevens wordt de keuze vrijheid voor toekomstige veranderingen vergemakkelijkt. Middelen worden alleen ingezet voor functies waarvoor zij bedoeld zijn. Andere inzet levert op korte of langere termijn mogelijk problemen in continuïteit / schaalbaarheid of functionaliteit op. Indien mogelijk worden middelen geselecteerd die voorbereid zijn op veranderingen in communicatiekanalen en gebruikers( organisaties).  De Best-of-suite benadering beoogt vermindering van de integratielast. |
| Consequenties | UWV houdt oog op relevante ontwikkelingen in de overheid en de ICT-markt en draagt daar hier op overheidsniveau eventueel aan bij. De ontwikkelingen worden doorvertaald in de roadmaps van de veranderingen op ICT –gebied. |

|  |  |
| --- | --- |
| P8 Inrichting IV gericht op voorkomen onjuist gebruik van gegevens | |
| Toelichting: | Systemen en gegevens worden beveiligd conform de eisen gesteld in het UWV tactisch beveiligings- en privacy beleid. Dit houdt bijvoorbeeld in dat gegevensvertrekking alleen wordt gedaan vanwege doelbinding, dat privacy- en medisch gevoelige gegevens worden beschermd en dat fraude wordt geïdentificeerd en voorkomen door logging en identiteit management. Voor levering van gegevens buiten UWV wordt de ongeautoriseerde toegang tot en inzage in de gegevens voorkomen. De IV garandeert dat het handelen van UWV t.a.v. zijn wettelijke taken op hoofdlijnen is te reconstrueren voor juridische verantwoording.  Verwijdering van overheidsinformatie uit de IV vindt plaats door geautoriseerde personen en volgens het vastgestelde protocol |
| Rationale: | UWV gaat om met heel persoonlijke, waaronder medische en financiële, gegevens. Deze gegevens kunnen worden gebruikt voor andere doeleinden dan waarvoor zij wettelijk zijn ingewonnen of gecreëerd. Nieuwsgierigheid maar ook frauduleuze motieven kunnen hieraan ten grondslag liggen. UWV heeft als taak om rechtmatig te handelen en daarover verantwoording af te leggen. De IV-functie maakt het mogelijk om de uitgevoerde activiteiten en beslissingen t.a.v. klantzaken, inkooptrajecten, etc. af te leiden, en deze voor te leggen als juridisch bewijs. |
| Consequenties | Maatregelen op zowel organisatorisch als technisch niveau dienen samenhangend te worden ontwikkeld en geïmplementeerd om fraude waar mogelijk te voorkomen en/of frauduleuze activiteiten te kunnen opsporen. Dit geldt voor zowel de UWV/SUWI-keten medewerkers als UWV klanten. |

## Afbakening RDT

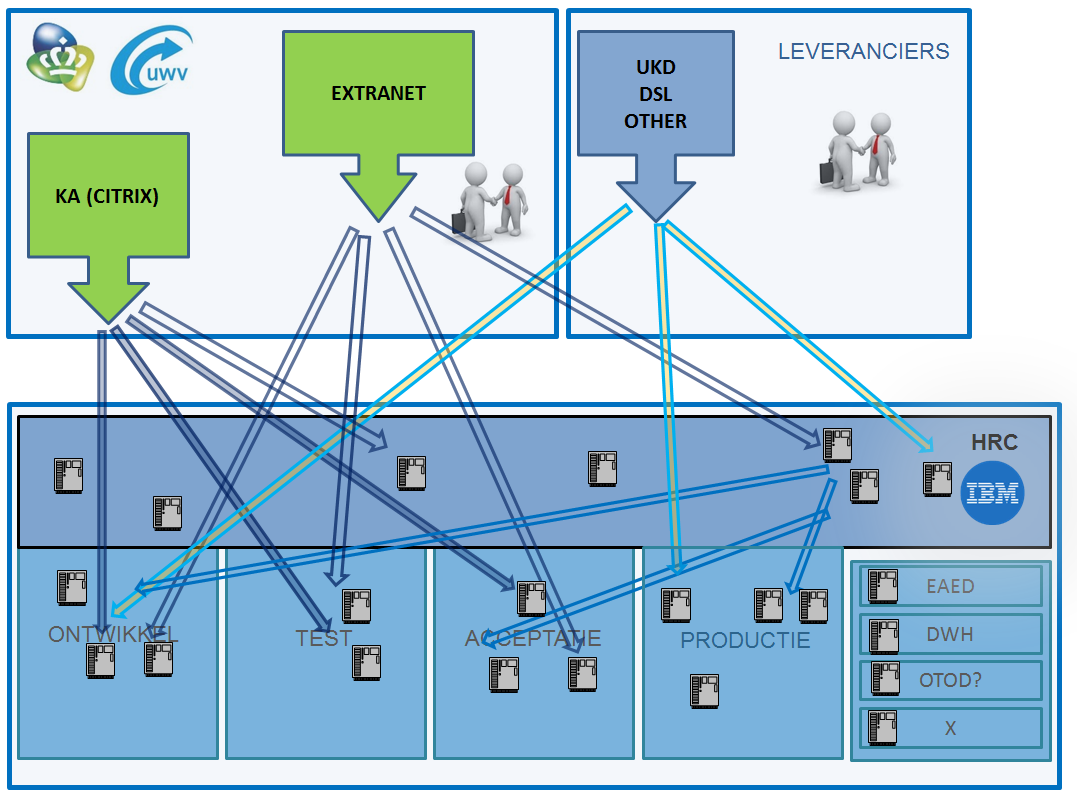
Dit beleidsdeel richt zich op de toegangsbeveiliging vanuit het RDT optiek. Het behandelt niet de inrichting van het managementsegment of de beschrijving van de softwarevoorzieningen (tooling) die buiten de applicatiefuncties in gebruik zijn. Het gebruik van toegang via RDP voor beheer doeleinden is in een ultieme situatie een onwenselijke voorziening. Het liefst zien we toegang tot de applicatie geregeld via applicatiefuncties waaraan gebruikers gekoppeld zijn. In de diversiteit van het UWV ICT landschap is het nodig gebleken om buiten de applicatie om toegang te verlenen, onder andere voor uitvoering van ontwikkel-, test of beheerwerkzaamheden. Om die toegang te verstrekken worden RDP servers gebruikt. Een RDP omgeving biedt in vele gevallen toegang tot applicatieservers en informatie welke vanuit de gestandaardiseerde UWV werkplek normaliter niet benaderbaar is.

Naast de bestaande centrale Remote Desktop Toegang (RDT) omgeving zijn er in de loop der jaren vele nieuwe verschillende remote desktop servers in gebruik genomen voor applicatie-specifieke doeleinden. De huidige situatie kent o.a. een risico t.a.v. de toegangslogging en het identity management.

Een goed ingerichte en beheerde centrale RDP omgeving lost een groot deel van de beveiligingsproblematiek op.

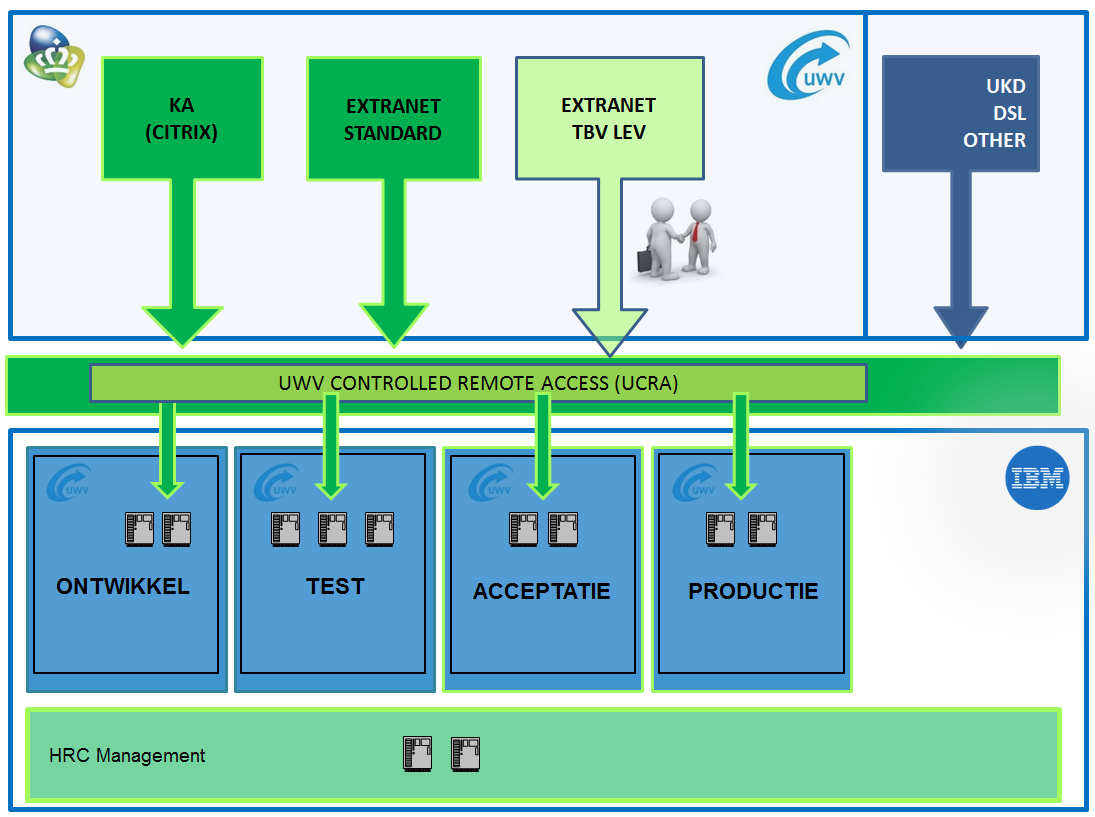
## Positionering en inrichting RDT

RDT is gepositioneerd in het managementsegment. UWV heeft gekozen voor een centrale inrichtring van het managementsegment. In dat centrale segment (zie tekening) zijn de voorzieningen – applicaties - geplaatst waarmee toegang mogelijk wordt voor medewerkers die de materieapplicatie dienen te benaderen. Deze toegang kan nodig zijn omdat de betreffende materieapplicatie niet beschikt over functies die noodzakelijk zijn voor onderhoud en beheer. Het onderstaande plaatje geeft weer



UWV maakt gebruik van een *centraal* managementsegment. Daarmee kunnen acties worden gelogd en kan toegang worden gecontroleerd. Zoals uit het plaatje ook blijkt levert een centraal management segment waarin de RDT is geregeld geen garanties voor het gebruik over de omgevingen heen. In de praktijk zien we dit ook gebeuren. Vanuit 1 en dezelfde server kunnen verschillende OTAP omgevingen worden benaderd door 1 en dezelfde gebruiker.

Voorkeur heeft het onderstaande plaatje waarin de stringente scheiding tussen de OTAP segmenten beter wordt geborgd. Toegang wordt verleend aan een persoon op basis van rechten die horen bij een rol. Daarmee wordt het principe dat Inrichting IV gericht is op voorkomen onjuist gebruik van gegevens beter geborgd. Het centrale managementsegment wordt in deze situatie alleen nog gebruikt voor generieke functies als licentiemanagement of software distributie.



## ICT Strategie & Beleid

Het document ‘ICT Strategie & Beleid’, opvolger van ‘IT Beleid en Strategie (2010)’ is bij de totstandkoming van deze richtlijn nog niet formeel vastgesteld. Als gevolg is er voor wat betreft OTAP, als onderdeel van ICT Strategie & Beleid en de UWV sourcingstrategie, nog geen formeel kader gedefinieerd. In dit document wordt nadere invulling gegeven aan IV principe 8 ‘Inrichting IV gericht op voorkomen onjuist gebruik van gegevens’

|  |  |  |
| --- | --- | --- |
| ***B.03 Gescheiden omgevingen*** | | |
| Criterium  (wie en wat) | *Omgevingen voor het ontwikkelen, testen, accepteren van applicaties en de voor die applicaties noodzakelijke infrastructuur zijn* ***gescheiden*** *van de productieomgevingen.* | *BIR 10.1.4*  *10.3.2* |
| Doelstelling (waarom) | *Productieomgevingen worden aangeboden aan (eind)gebruikers. De overeengekomen serviceniveaus worden bewaakt en de regelgeving op het gebied van de informatiebeveiliging wordt gerespecteerd.* |  |
| ***Gescheiden omgevingen*** | | |
| 01 | Productieomgevingen bevinden zich op gescheiden (virtuele) machines, in een apart(e) netwerksegment / -zone die niet direct toegankelijk is vanaf andere OTA-omgevingen. | BIR 10.1.4.2 |
| 02 | Productieomgevingen mogen niet worden verstoord / beïnvloed door test- of ontwikkelwerkzaamheden. | BIR 10.1.4.1 |
| 03 | Er worden geen testactiviteiten uitgevoerd op de productieomgeving. |  |
| 04 | Gescheiden omgevingen voor het ontwikkelen, testen en accepteren biedt de mogelijkheid in iedere fase van OTAP representatieve tests uit te voeren zonder andere omgevingen te verstoren. | BIR 10.1.4.1 |
| 05 | Acceptatieomgevingen zijn qua inrichting van de infrastructuur, hardware en software nagenoeg identiek aan de productieomgevingen. | BIR 10.3.2 |

# Uitvoeringsdomein

De volgende paragraven gaan over de daadwerkelijke invulling van de beleidsrichtlijnen.

## Doelstelling

De doelstelling van het uitvoeringsdomein is te waarborgen dat de inrichting van RDT voorzieningen overeenkomstig algemene en specifieke beleidsuitgangspunten plaatsvindt en dat de werking voldoet aan de eisen die door UWV op basis van het RDT-beleid zijn gesteld.

In de beschrijving van essentiële normen en voorwaarden voor een veilig gebruik van RDT voorzieningen staan bedrijfsbelang en risico-inschatting centraal bij het invullen van de in de volgende paragrafen benoemde aandachtsgebieden.

Voor alle elementen in de beschrijving geldt dat deze contractueel dienen te worden vastgelegd in een schriftelijke overeenkomst tussen UWV en de dienstverlener.

## Toegang

|  |  |  |
| --- | --- | --- |
| **U.01 Clientserver toegang tot OTAP** | | |
| Criterium (wie en wat) | **Clientserver** toegang tot de **productiezone** is toegestaan aan **productiegebruikers**. |  |
| Doelstelling (waarom) | Clientserver toegang tot de productiezone in een UWV rekencentrum en de daarbinnen gehoste omgevingen en systemen (applicaties) is altijd toegestaan aan geautoriseerde productiegebruikers met een (virtuele) werkplek waarop de noodzakelijke clientsoftware en middleware is geïnstalleerd. |  |
| **U.02 Web-based toegang tot OTAP** | | |
| Criterium (wie en wat) | **Web-based** toegang tot de **OTAP-zones** is toegestaan aan alle **gebruikers**. |  |
| Doelstelling (waarom) | Web-based toegang tot alle OTAP zones in een UWV rekencentrum en de daarbinnen gehoste omgevingen en systemen (applicaties) is altijd toegestaan aan geautoriseerde gebruikers met een (virtuele) werkplek waarop een browser is geïnstalleerd | |
| **U.03 Toegang testgebruikers** | | |
| Criterium (wie en wat) | **Testgebruikers** hebben **rechtstreeks** toegang tot de acceptatie- en ontwikkel/testzone, **tenzij**. |  |
| Doelstelling (waarom) | Geautoriseerde testgebruikers hebben rechtstreeks toegang tot de acceptatie en ontwikkel/testzone in een UWV rekencentrum en de daarbinnen gehoste omgevingen en systemen (applicaties) tenzij de toegang een aanpassing van de (virtuele) werkplek noodzakelijk maakt. In dat geval is het gebruik van in de in het UWV HRC gehoste Remote Desktop (of soortgelijke) voorziening vereist. |  |
| **U.04 Toegang testers en ontwikkelaars** | | |
| Criterium (wie en wat) | **Testers** en **ontwikkelaars** hebben enkel toegang tot de acceptatiezone via de **RDP area** in de managementzone. |  |
| Doelstelling (waarom) | Geautoriseerde testers en ontwikkelaars hebben zonder uitzondering via de in een UWV Rekencentrum gehoste Remote Desktop (of soortgelijke) voorziening toegang tot de ontwikkel/testzone en de daarbinnen gehoste omgevingen en systemen (applicaties). DE benodigde applicaties of tools staan evenwel niet op het RDP segment maar in de betreffende omgeving |  |

|  |  |  |
| --- | --- | --- |
| **U.05 Toegang softwarebouwers met een UWV account** | | |
| Criterium (wie en wat) | **Softwarebouwers met een UWV account** hebben enkel toegang tot de ontwikkel/testzone via de **RDP area** in de managementzone. |  |
| Doelstelling (waarom) | Softwarebouwers met een UWV account (geautoriseerd) hebben zonder uitzondering via de in een UWV Rekencentrum gehoste Remote Desktop (of soortgelijke) voorziening toegang tot de ontwikkel/testzone en de daarbinnen gehoste omgevingen en systemen (applicaties). Speciale tooling en / of noodzakelijke aanpassing van de werkplek (clientsoftware, middleware et cetera) worden geleverd op de (virtuele) Remote Client. |  |
| **U.06 Toegang softwarebouwers zonder een UWV account** | | |
| Criterium (wie en wat) | **Softwarebouwers zonder een UWV account** hebben enkel toegang tot de **eigen ontwikkel- en/of testzones**. |  |
| Doelstelling (waarom) | Softwarebouwers zonder een UWV account hebben zonder uitzondering alleen toegang tot de in een eigen rekencentrum gesitueerde ontwikkel- en/of testzones en de daarbinnen gehoste omgevingen en systemen (applicaties). |  |
| **U.07 Toegang functionele beheerders tot productiezone** | | |
| Criterium (wie en wat) | **Functionele beheerders** met (extra) tooling hebben enkel toegang tot de productiezone via de **RDP area**. |  |
| Doelstelling (waarom) | Functionele beheerders met speciale tooling, rechten en/of noodzakelijke aanpassing van de (virtuele) werkplek hebben zonder uitzondering enkel via de gehoste Remote Desktop (of soortgelijke) voorziening toegang tot de in een UWV rekencentrum gesitueerde productiezone en de daarbinnen gehoste omgevingen en systemen (applicaties). |  |
| **U.08 Toegang applicatiebeheerders tot productiezone** | | |
| Criterium (wie en wat) | **Applicatiebeheerders** hebben toegang tot de productiezone via de **RDP area**. |  |
| **U.10 Externe toegang tot het UWV domein** | | |
| Criterium (wie en wat) | Externe toegang tot het (netwerk)**domein van UWV** is, mits **geauthentiseerd / geautoriseerd**, toegestaan via de UKD. |  |
| Doelstelling (waarom) | Toegang vanuit een extern domein tot systemen in de verschillende zones van het UWV domein is niet toegestaan, tenzij de geauthentiseerd / geautoriseerd in de UKD. In dat geval wordt de externe partij als UWV medewerker beschouwd en krijgt die toegang conform de rechten die aan het toegekende account zijn gegeven. Daarbij geldt dat de platformleverancier van het rekencentrum verantwoordelijk is voor de (toegangs)beveiliging. Ook voor de inregeling van de logische toegangsbeveiliging waarin de rechten zijn geregeld. |  |

## Communicatie en koppelingen

Onder communicatie verstaan we de uitwisseling van data tussen de OTAP segmenten

|  |  |  |
| --- | --- | --- |
| **U.12 Communicatie tussen OTAP-zones** | | |
| Criterium (wie en wat) | **Communicatie** tussen verschillende **OTAP-zones** is **conditioneel** / beperkt toegestaan via de managementzone. |  |
| Doelstelling (waarom) | De OTAP-zones en de daarbinnen gehoste omgevingen en systemen (applicaties) zijn door de rekencentrumleverancier(s) zodanig van elkaar gescheiden dat niet geautoriseerde communicatie (verkeersstromen) onderling niet mogelijk zijn. |  |
| ***Communicatie*** | | | |
| 01 | Communicatie van softwareaanleveringen verloopt via de staging area |  | |
| ***OTAP-zones*** | | | |
| 02 | OTAP-zones / omgevingen kunnen ook buiten de UWV rekencentra voorkomen. Bijvoorbeeld in het subdomein van de werkplekken / locaties of bij externe software- / applicatieleveranciers. |  | |
| ***conditioneel*** | | | |
| 03 | Bestandsoverdracht tussen VLAN’s is alleen mogelijk via voorzieningen in de managementzone in een UWV rekencentrum, waarbij bestanden worden gecontroleerd op kwaadaardige software. |  | |
| 04 | De categorie ‘werkplekken / locaties’, uitgezonderd de productiezone, is alleen toegestaan op uitdrukkelijk verzoek (exceptie), bijvoorbeeld wanneer de eisen van de client-servercommunicatie het gebruik van Remote Desktop Terminalemulatie niet toestaat. |  | |
| 05 | De categorie ‘externe software- / applicatieleveranciers’ betreft voornamelijk de ontwikkelomgeving(en) bij software- / applicatieleveranciers |  | |
| 06 | Een directe communicatie met het domein en de in dat domein gehoste zones / omgevingen van externe partijen is per definitie niet toegestaan |  | |
| 07 | Binnen / tussen zones van hetzelfde type, binnen één domein, is communicatie altijd toegestaan, met andere woorden: ze vormen één virtuele zone over het domein heen. |  | |
| 08 | Directe communicatie tussen zones van verschillend type is niet toegestaan en dient via de managementzone in het (lokale) rekencentrum te lopen. Dit geldt expliciet voor alle in de zone gehoste systemen / omgevingen. |  | |
| 09 | De ondersteunende infrastructuur / systemen, ook in de ontwikkel en testzones vallen onder het productieregime en communicatie tussen elementen van die infrastructuur is wel toegestaan. |  | |
| 10 | De communicatie tussen de management zone en de andere OTAP-zones is conditioneel / beperkt toegestaan voor de toegang middels Remote Desktop Terminalemulatie, software deployment / distributie en gegevensuitwisseling. |  | |

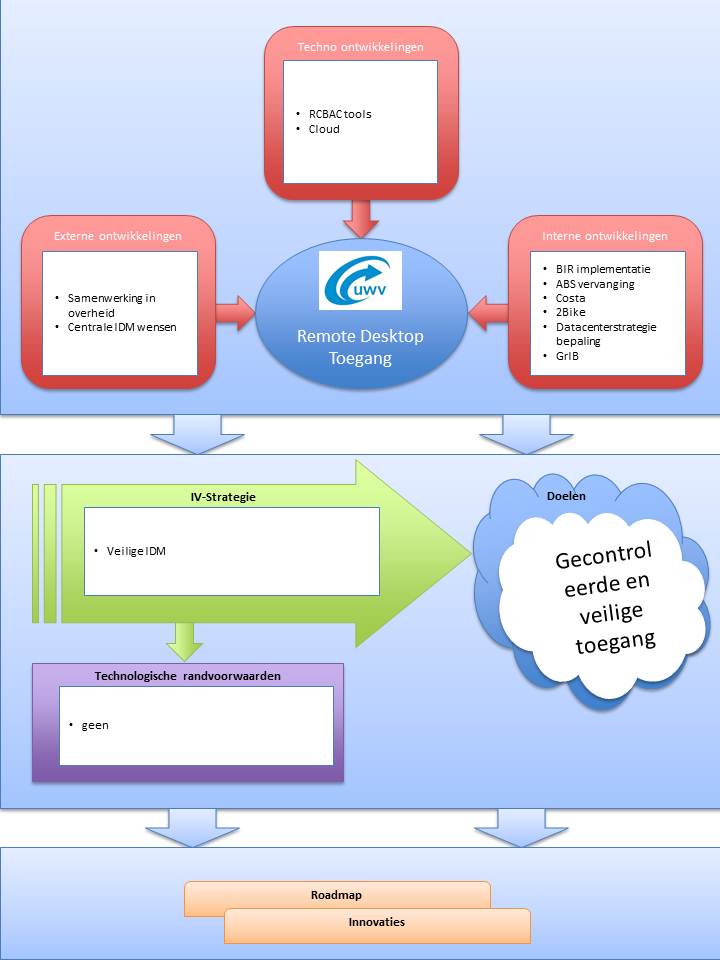
|  |  |  |
| --- | --- | --- |
| **U.13 Gegevensuitwisseling via de managementzone** | | |
| Criterium (wie en wat) | **Gegevensuitwisseling** gebeurt via de daarvoor ingerichte voorzieningen |  |
| Doelstelling (waarom) | Gegevensuitwisseling gebeurt via de daarvoor ingerichte voorzieningen |  |
| ***Gegevensuitwisseling*** | | |
| 01 | Dit betreft het koppelen van systemen en het uitwisseling van gegevens (file transfer) tussen die systemen / applicaties. |  |
| 02 | Onderlinge gegevensuitwisseling tussen systemen binnen een zone, binnen één of meer omgevingen, is zonder meer toegestaan. |  |
| 03 | Gegevensuitwisseling tussen systemen die in verschillende zones staan is slechts toegestaan wanneer gebruik gemaakt wordt van anonimiseringssoftware of middels specifiek geautoriseerde gebruikers. |  |
| 04 | Uitzondering is de gecontroleerde transfer van gegevens via de Data Staging Area in de managementzone. |  |
| 05 | De uitwisseling wordt altijd geïnitieerd vanuit één van de OTAP-zones, waarna gegevens naar een server in de managementzone kan worden verstuurd, of gegevens van die server kunnen worden opgehaald. |  |
| 06 | Alleen degene die toegang heeft tot een bepaalde omgeving (zone) kan vanuit die omgeving de file overzetten, maar dan uitsluitend op dat deel van de server waar overeenkomstige rechten van toepassing zijn. |  |
| 07 | Hiermee is het principe van functiescheiding toegepast en kunnen bestanden op kwaadaardige software worden gecontroleerd. |  |

|  |  |  |
| --- | --- | --- |
| **U.14 Softwaredistributie via de managementzone** | | |
| Criterium (wie en wat) | **Softwaredistributie** gebeurt altijd via de daarvoor ingerichte voorzieningen in de managementzone. |  |
| Doelstelling (waarom) | Softwaredistributie gebeurt altijd via de daarvoor ingerichte voorzieningen in de managementzone. |  |
| ***Softwaredistributie*** | | |
| 01 | Dit betreft het transporteren van ´ondersteunende´ software en software-updates, niet bijhorende tot de deployment van applicatie(releases). |  |
| 02 | Bijvoorbeeld patches, securityupdates et cetera. Het transport loopt via het softwaredistributieplatform in de managementzone. |  |

# RDT bij UWV

De context waarin RDT zich beweegt.

## Context



## Huidige situatie

In de huidige situatie vinden we Remote Desktop servers op verschillende plekken. De centrale managementzone is aanwezig en daarnaast staan er RDP servers in de diverse OTAP segmenten. Zoals aangegeven in de beleidstelling is een centrale managementvoorziening de enige plek waarin gecontroleerd toegang kan worden verleend aan applicaties.

Het gebruik van toegang via RDP voor beheer doeleinden is in een ultieme situatie een onwenselijke voorziening. Het liefst zien we toegang tot de applicatie geregeld via applicatiefuncties waaraan gebruikers gekoppeld zijn. In de diversiteit van het UWV ICT landschap is het nodig gebleken om buiten de applicatie om toegang te verlenen. Daartoe is het Remote Desktop Toegang omgeving in het leven geroepen. In de loop der jaren zijn er vele nieuwe verschillende remote desktop servers in gebruik genomen waar eigenlijk een beperkt aantal zou volstaan. De huidige situatie kent o.a. een risico t.a.v. de toegangslogging en het Identity Management.

## Gewenste situatie

Gebruik de RDT omgeving alleen om toegang te verlenen en plaats de diverse softwarematige voorzieningen in de diverse OTAP segmenten. Daarmee wordt het gebruik van deze producten ook gereguleerd tot de fases waarvoor het bedoeld is. Bijvoorbeeld: het gebruik van TOAD in een O omgeving is toegestaan, echter op de P omgeving een ernstig beveiligingsrisico.

# Begrippen en definities

**RDP**

Remote Desktop Protocol, dit is het protocol gebruikt door de Microsoft Remote Desktop cliënt waarmee vanaf een Windows computer een andere Windows computer kan worden benaderd in een remote desktop sessie.

**RDT**

Remote Desktop Toegang, dit is een bestaande centrale voorziening binnen het UWV HRC, bestaande uit meerdere RDP servers.

**ESA**

Eenduidige Software Aanlevering, dit is een transportmiddel en repository voor de aanlevering van maatwerksoftware door applicatieleveranciers van UWV

**VLAN**

Virtual LAN, dit is een netwerk dat logisch gescheiden is van andere netwerken op hetzelfde fysieke LAN

**UKD**

UWV Koppel Dienst, dit is een dienst waarmee vertrouwde externe partijen aan het UWV netwerk kunnen koppelen door middel van bijvoorbeeld VPN verbindingen.

**Managementsegment of managementzone**

Één van de VLANs die UWV kent, ingericht ten behoeve van centrale voorzieningen als RDT, licentieservers etc.

## 