Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Producten en Diensten Catalogus Netwerken CIV

Ten behoeve van externe afnemers

Uitgegeven door:

Service Portfolio Manager	Conclusion Operationele Service Integrator (OPSI)
Service Portfolio Manager	RWS CIV IRN INFRA NETWERKEN

Datum:	01-05-2025
Status:	Definitief
Classificatie:	Conclusion Vertrouwelijk, RWS Bedrijfsinformatie
Versie: 21.0	

Contents

Documentbeheer **2**
Documentversies 3

Inleiding **3**
Relatie met andere documenten 4
Dienstverlening RWS CIV IRN Infra Netwerken 4

Netwerkdiensten CIV Afnemer **6**

Netwerkdiensten CIV Afnemer **8**
Inleiding 8
Categorie VPN 8
Categorie VPN aansluiting 12
Categorie LAN aansluiting 27
Categorie Eindsystemen 38
Categorie Overig 47
Beheren IT-netwerkdiensten (Specials) 52
Verbindingen Lichteiland Goeree – Europlatform 52
CCM aansluiting 52

Totaal overzicht SLA Matrix **53**

Bijlage A Afkortingen en Begrippen **54**

Bijlage B Overzicht tabellen **58**

Bijlage C Overzicht figuren **59**

Documentbeheer

Documentversies

Eigenaar	Datum	Versie	Samenvatting van de wijziging	Status
KPN DO RWS		1 tm 19	Diversen, zie versie 20 voor details	
KPN DO RWS	31-03-2025	20	1. Loggingdienst: verwachte realisatie van de techniek, om zodoende herstelgaranties op de dienst te kunnen geven, is aangepast naar 2026. 2. Beheerverbindingen LEG-EPL: Servicelevel aangepast naar E8. 3. Categorie Special: Noodknopbediening Sijtwendetunnel uit dienstenportfolio verwijderd. 4. Toevoegen Hub Spoke als bestelbare optie op draadloze VPN aansluiting	Definitief
Conclusion OPSI	01-05-2025	21	1. Nieuw bronbestand met overzicht leveringen (eigenaar RWS ESI) verwerkt 2. Structuur document herzien als onderdeel van de Transitie naar nieuwe leverancier 3. Overgezet naar RWS huisstijl Splitsing in drie documenten: 1. Geconsolideerde technische service catalogus BOSI 2. PDC versie 21 tbv RWS infra 3. PDC versie 21 tbv externe afnemers (alleen deel 2)	Definitief

Inleiding

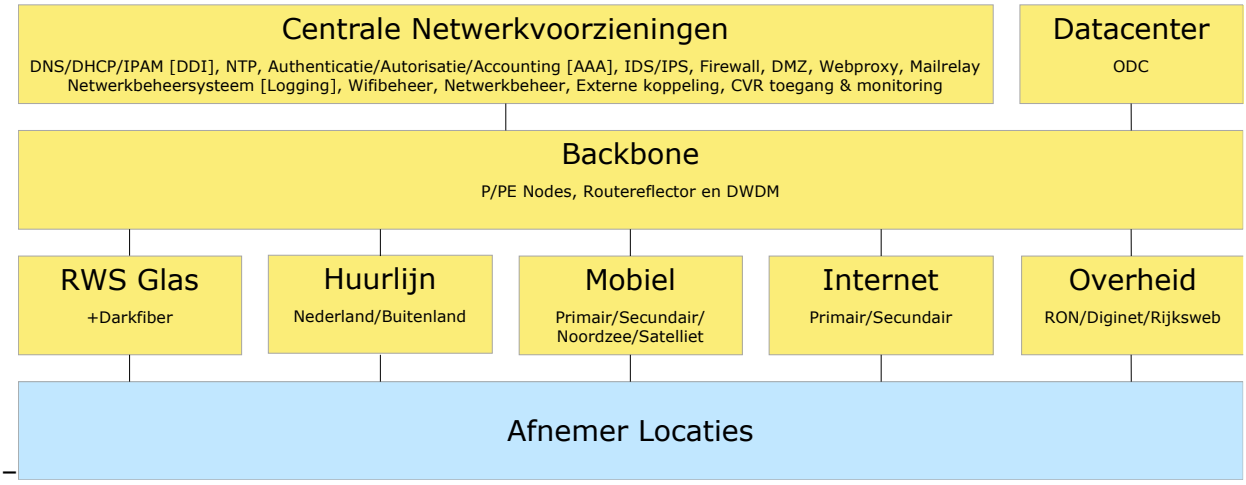
Doel van deze catalogus is het bieden van een overzicht van de diensten die RWS CIV IRN Infra Netwerken op netwerkgebied afneemt van de Service Providers en welke RWS CIV IRN Infra Netwerken biedt aan haar afnemers.

Relatie met andere documenten

Document	Eigenaar	Versie	datum
Afnemer Netwerkdiensten Wizard	ESI	1.0	01-05-2025
Technische Service Tree	OPSI	1.0	01-05-2025

Dienstverlening RWS CIV IRN Infra Netwerken
Algemeen
Rijkswaterstaat Centrale Informatievoorziening (CIV) zorgt voor de ontwikkeling en beschikbaarheid van informatie binnen Rijkswaterstaat. CIV zorgt voor industriële automatisering bij bruggen, tunnels, rijkswegen en andere objecten. Daarnaast verzorgt CIV de kantoorautomatisering. RWS CIV IRN Infra Netwerken draagt binnen RWS CIV zorg voor de netwerkinfrastructuur en bijbehorende dienstverlening.

Scope
RWS CIV IRN Infra Netwerken is verantwoordelijk voor het beheer, project- en contractmanagement van haar netwerkomgeving. De uitvoering hiervan is belegd bij de outsourcingspartner Conclusion Quanza.



Figuur 1 Scope IT-netwerkdiensten

De netwerkdienstverlening beslaat de volgende domeinen:
- RWS netwerk;
- LAN voor Kantoorautomatisering (KA);
- Object Access Netwerken:

  - Netwerken die worden gebruikt om objecten, binnen Rijkswaterstaat ook wel kunstwerken genoemd, maar ook systemen langs weg- en waterwegen, te ontsluiten;
- De WAN verbindingen naar Locaties (kantoren en rekencentra), wegkantsystemen, verkeerscentrales, objecten zoals bruggen, sluizen en tunnels en losse huurlijnen.
- Koppelingen met externe netwerken (internet, mobiel, de Haagse Ring, RON2.0 e.a.);
- Functieherstel glasvezelnetwerk:
  - Herstellen van verstoringen op RWS glasvezels;
  - Glasvezelbeheer (o.a. vezelbezetting en uitgifte van vezels).

Uitvoeren Operationele ITIL-diensten
De uitvoering van de verschillende ITIL-diensten is beschreven in het Ketenhandboek IT-netwerkdiensten. Hierin staan alle generieke afspraken binnen het ecosysteem van de IT-netwerkdiensten beschreven. Daarnaast bestuurt OPSI de verschillende service providers in de keten ondersteund door specifieke afspraken die zijn beschreven in Operational Level Agreements (OLA's). In dit hoofdstuk worden de belangrijkste afspraken, die relevant zijn voor de interne en externe afnemers van de dienstverlening, samengevat.

Service Control Center (SCC)
Ten eerste verwerkt de OPSI SCC, als centrale spil, alle vragen, orders en storingsmeldingen van de afnemers van de Rijkswaterstaat organisatie. Hierbij worden via een gecontroleerd proces de diverse toeleveranciers en derde partijen aangestuurd. Ten tweede verricht de SCC alle noodzakelijke registraties ten behoeve van terugkoppeling, rapportage, bijsturing en facturering.
Het SCC vormt een integraal onderdeel van de OPSI dienstverlening en omvat de volgende functies:
- Helpdesk: Ondersteunen van de medewerkers/afnemers van Rijkswaterstaat bij vragen over afgenomen diensten;
- Orderdesk: Ingang waar geautoriseerde personen opdrachten en eenmalige diensten (Install, Move, Add en Change (IMAC's)) indienen;
- Melddesk: Voor het melden van storingen, incidenten en klachten.

Het SCC beantwoordt de vragen van Rijkswaterstaat. Als het SCC de vragen niet kan beantwoorden wordt contact gezocht met de achterliggende supportgroepen of derde contractpartijen om tot een antwoord te komen. Hierover zijn afspraken gemaakt met de achterliggende partijen.
Het SCC is 24x7 zowel telefonisch als per e-mail bereikbaar:
- Incidenten kunnen 24x7 telefonisch gemeld worden en worden conform geldende SLA afspraak afgerond;
- De afhandeling van orders zal plaatsvinden tijdens kantooruren;
- Informatievragen kunnen 24x7 per e-mail gesteld worden. Tijdens kantooruren kunnen deze vragen ook telefonisch gesteld worden. De afhandeling van informatievragen vindt plaats tijdens kantooruren.

Service Providers

CCMKO	Contact Center Missie Kritieke Ondersteuning
KA Service Desk	Service Desk KA-omgeving, on site support op grote kantoorlocaties
OPSI	Operationele integratie van de IT-netwerkdiensten
IB	Integraal Beheer van het RWS netwerk
O&A	Onderhouden en Aanpassen van IT-netwerkdiensten
SPIE	Field Services – diverse werkzaamheden op locatie ten behoeve van Beheer, Onderhoud en Aanpassen; voorraadbeheer netwerk hardware
Odido	Vaste data huurlijnen, Mobiele SIM-kaarten (backup)
Vodafone	Mobiele SIM-kaarten (primair)
ProximusNXT	Bestelling en levering Cisco Hardware

Bestellingen
Deze catalogus beschrijft de standaard bestelbare diensten van CIV IRN Infra Netwerken. Afnemers kunnen zonder tussenkomst van CIV IRN Infra Netwerken een standaard levering aanvragen. Levervragen die (nog) niet met de standaard Product en Diensten Catalogus kunnen worden ingevuld worden On hold geplaatst tot een ontwikkeling van een standaard bestelbaar item door CIV IRN Infra Netwerken is afgerond. Indien levering vooruitlopend op ontwikkeling noodzakelijk is, kan met de PDC Uitzonderingen Procedure toestemming gevraagd worden om op basis van een PDC Exceptie de levering op te starten parallel aan een ontwikkeltraject.

Verstoringen
Indien een verstoring van een IT-netwerkdienst optreedt, dient contact opgenomen te worden met de eerstelijns service desk. Vanuit een kantooromgeving is dat de KA Service desk, voor verstoringen 'in het veld' wordt contact opgenomen met het CCMKO. Indien zij constateren dat het een storing van de IT-netwerkdiensten betreft dan wordt het SCC van de OPSI aangestuurd.

Ten behoeve van het oplossen van verstoringen stuurt de OPSI, afhankelijk van het type verstoring, één of meerdere service providers aan. Als er assistentie op locatie nodig is zijn er twee opties:

- On site support door KA Service Desk, voor het initieel nadere informatie verzamelen over de verstoring;
- Field Services door SPIE voor alle andere benodigde activiteiten op locatie.

Netwerkdiensten CIV Afnemer

VPN (functionaliteiten)
VPN
Virtual Firewall
DDI

DMZ
Forward Webproxy
Mail Relay
VPN Aansluiting
VPN aansluiting
Draadloze VPN aansluiting
Externe koppeling
LAN Aansluiting
LAN aansluiting type Gebouw
LAN aansluiting type Rekencentrum (VC/VP)
LAN aansluiting type CVR/VOR
LAN aansluiting type Weg- / Waterkant
LAN aansluiting type Onderstation
LAN aansluiting type Offshore
LAN aansluiting type KA, incl. callcenter
WIFI
Eindsysteem
Digitale Video aansluiting
Remote Access groepsprofiel
AAA RAS gebruiker
AAA NAC Profiel
PPP aansluiting
TBMS BUS
Draadloze aansluiting
Overig
Glas Adviezen, Netwerk Adviezen

Tabel 1 IT-netwerkdiensten CIV Klant

Netwerkdiensten CIV Afnemer

Inleiding
Deze catalogus biedt een overzicht van de diensten welke door afnemers van CIV IRN Infra Netwerken kunnen worden besteld in de categorie VPN, VPN Aansluiting, LAN Aansluiting en Eindsysteem.

Categorie VPN
Onder de categorie Virtual Private Network (VPN) vallen het VPN en de additionele functionaliteiten op het VPN zoals DDI, DMZ en DMZ Client, Mail Relay en de Virtual Firewall. Om gebruik te kunnen maken van verscheidene functionaliteiten uit de categorieën Eind-systemen, LAN aansluiting en VPN aansluiting wordt gebruik gemaakt van een VPN. De aan-vrager dient aan te geven op welk VPN hij aangesloten wenst te worden.

Virtual Private Networks (VPN's) zijn landelijk beschikbaar en kunnen middels de diensten VPN aansluiting en LAN aansluiting tot op LAN access poort niveau op eindlocaties ontsluiting bieden tot systemen. Optioneel kan het VPN via een Virtual Firewall verbonden worden met andere VPN's en met het internet. Afhankelijk van het type VPN zijn bepaalde standaardvoorzieningen mogelijk, verplicht of beperkt. Het VPN is in twee varianten te bestellen; het any-to-any VPN en het Hub-Spoke VPN. De infra adviseur ondersteunt de besteller bij het maken van de keuze voor een van de types.

VPN any-to any
In dit type VPN is er binnen het VPN transparante communicatie mogelijk tussen alle locaties die aangesloten zijn op het betreffende VPN.

VPN Hub-Spoke
In een Hub-Spoke VPN is rechtstreekse communicatie tussen locaties (zgn. Spokes) uitgesloten. Een VPN aansluiting Spoke kan enkel met de Hub of met externe VPN's communiceren via een Firewall. Dit type VPN is met name bedoeld voor netwerkomgevingen waar verhoogde veiligheid voorop staat. Multicast wordt in een Hub-Spoke VPN niet ondersteund.

De Hub-Spoke functionaliteit is te bestellen door een combinatie van de volgende diensten:
- VPN type Hub-Spoke
- VPN aansluiting type Hub (locatie Primair/Secundair verplicht aangeven wanneer het een CV of ODC locatie betreft)
- VPN aansluiting type Spoke
- VPN FW Policy&Rules

Per VPN type Hub-Spoke worden één of meerdere Spoke aansluitingen en één Hub-functie ondersteund. De Hub-functie is redundant te leveren over twee geografisch gescheiden locaties (primair/secundair). De Hub functie is alleen leverbaar op de locaties Centrale Voorzieningen, ODC en Verkeerscentrales.

Wanneer eenmaal voor een type VPN is gekozen, any-to-any of Hub-Spoke, dan is er geen migratie naar een ander type mogelijk. Er kan alleen naar een ander type worden overgestapt dmv bestellen van de activiteiten ''opheffen'' van het bestaande type VPN en ''aanvragen'' van het gewenste type VPN.

Een VPN biedt de mogelijkheid binnen een besloten en logisch gescheiden netwerk op veilige, betrouwbare wijze bedrijfsinformatie en applicaties te benaderen én informatie te delen tussen geografisch gescheiden netwerken als binnen één dedicated netwerk. Het VPN is rand-voorwaardelijk om communicatie tussen eindsystemen op twee RWS locaties en tussen RWS en niet-RWS eindlocaties mogelijk te maken. Afhankelijk van het doel van het VPN dienen de in onderstaande tabel weergegeven functionaliteiten verplicht of optioneel afgenomen te worden om gebruik te maken van de diensten beschreven in de categorieën Eindsystemen, LAN aansluiting en VPN aansluiting.

VPN functionaliteiten		
Functionaliteit	**Standaard / Verplicht/Optioneel**	**Specificatie**
Managed IP-VPN	Standaard	Any to any, of Hub Spoke, IP connectiviteit tussen op de RWS backbone ontsloten locaties. Routering binnen een virtueel netwerk in de RWS backbone met een door de beheerder SP-IB toegewezen IPv4-adresruimte
Externe koppeling	Optioneel	In- en/of uitgaand verkeer naar aangesloten externe netwerken (Categorie VPN Aansluiting)
Internet Access met gefilterd Internet	Standaard	Veilige en gecontroleerde toegang tot het Internet voor in- en/of uitgaand internet verkeer voor interactie met partijen buiten de RWS organisatie.
Virtual Firewall	Verplicht	Beschermt de integriteit en vertrouwelijkheid van het VPN middels een firewall. De Virtual Firewall bepaalt per VPN welke communicatiestromen zijn toegestaan en blokkeert alle niet expliciet toegestane communicatie(patronen). Ieder VPN heeft een eigen Virtual Firewall.
IDS/IPS	Standaard	IDS controleert het verkeer tussen VPN's en van en naar het Internet op schadelijke aspecten en IPS blokkeert volgens ingestelde policies.
Mail Relay	Optioneel	Benodigd om e-mail te ontvangen van en versturen naar externe netwerken via smtp protocol. Mail Relay heeft daarbij verschillende beveiligingsvoorzieningen zoals controle op de reputatie van een systeem op Internet, versleuteling van email transport en inhoudelijke controle van berichten.
DNS (DDI)	Verplicht bij Internet Access	De functie DNS levert 'name services' aan de, binnen het VPN, aangesloten systemen op basis van het DNS protocol en voorziet in DNS name resolving van Internet systemen.

DHCP (DDI)	Standaard	De functie DHCP levert een centrale voorziening om clients (en hosts) binnen het VPN op dynamische wijze van netwerkinstellingen te voorzien middels DHCP (Dynamic Host Configuration Protocol)
IPAM (DDI)	Standaard	Address Management geeft geautoriseerde RWS medewerkers de mogelijkheid om de IP-gerelateerde informatie vast te leggen en hier context aan te geven. Zo wordt IP-informatie beter bruikbaar als ondersteuning bij audits, kwaliteitscontrole en incidenten.
Gedelegeerd beheer (DDI)	Standaard	Geeft RWS medewerkers en RWS onderaannemers de mogelijkheid om de 'IP-ruimte' waarvoor zij verantwoordelijk zijn te beheren.
Remote Access	Optioneel bij Internet Access	Remote Access door personen (Internet) naar RWS systemen ten behoeve van remote beheer.
QoS	Optioneel	Congestiebeheersing door end to end Quality Of Service (QoS) binnen een VPN. QoS is niet overal en altijd leverbaar.
NTP	Standaard	De functie NTP levert een centrale klok waarmee eindsystemen binnen het VPN hun tijd kunnen synchroniseren via het NTPv4 protocol.

Tabel 2 VPN functionaliteiten

Beheer VPN

RWS onderkent de volgende onderdelen van de categorie VPN:

1. VPN
2. Virtuele Firewall
3. DDI – DHCP & DNS
4. DDI – IPAM
5. DDI – Gedelegeerd beheer
6. DDI – NTP
7. DMZ en DMZ client
8. Forward Webproxy
9. Mail Relay

Quanza IB voert het beheer uit op deze VPN types conform onderstaande SLA.

MATRIX VPN											
Diensten	Beschikbaarheid							Storingshersteltijd in 95% van de gevallen			
	Enkel			Dubbel			VPN	Service Window Kantoortijden		Service Window"24/7"	
	99,5%	99,9%	99,95%	99,98%	99,99%	99,99%	99,999%				
	Onbeschikbaarheid per jaar										
	ca 1d20u	ca 8u45m	ca 4u28m	ca 4u28m	ca 1u45m	ca 0u52m	ca 5m15s	8 uur	4 uur	8 uur	4 uur
VPN							V				V
Virtual Firewall			V								V
DDI- DHCP & DNS*	V					V					V
DDI- IPAM		V									V
DMZ en DMZ Client					V						V
Forward Webproxy				V							V
Mail Relay				V							V

* De centrale beschikbaarheid van DDI componenten is 99,99%, deze zijn dubbel uitgevoerd en hiertoe geplaatst over 2 fysiek geografisch gescheiden locaties. De beschikbaarheid over de gehele keten is afhankelijk van de overige bouwstenen waar de afnemer gebruik van maakt.

Tabel 3 Dienstenmatrix VPN – diensten

Bestelbare items en levertijd

Voor het VPN gelden de in onderstaande tabel weergegeven bestelbare items met bijbehorende standaard in werkdagen weergegeven levertijden. De levertijden voor verschillende bestelbare items lopen parallel, niet sequentieel. De dienst VPN is niet apart door afnemers te bestellen.

VPN			
nmalige dienst	**Toelichting**	**evertijd in werkdagen oor SP-O&A)**	**SSR oor SP-IB)**
VPN			
Aanvragen	Leveren nieuw VPN	20	
Opheffen	Opheffen VPN	20	
Wijzigen	Wijzigen instelling bestaand VPN op afstand	10	
Aanvragen VPN QoS Profiel	Realiseren QoA profiel op VPN	20	
Virtual firewall			
Aanvragen	Leveren nieuwe Firewall	10	
Opheffen	Opheffen Firewall	10	
Wijzigen	Wijzigen/toevoegen/verwijderen Firewall rules	5	Ja
Wijzigen	Wijzigen/toevoegen/verwijderen Firewall rules met spoed	1	Ja
DDI – DHCP Scope			
Aanvragen	Aanvragen DHCP scope (IP range centrale distributie)	10	
Opheffen	Opheffen DHCP scope (IP range centrale distributie)	10	
Wijzigen	Wijzigen DHCP scope (IP range centrale distributie)	10	
Aanvragen toegang	Aanvragen toegang op bestaande DHCP scope RW/RO	10	
Opheffen toegang	Opheffen toegang op bestaande DHCP scope RW/RO	10	
DDI – DNS Domeinnaam			
Aanvragen	Leveren DNS domeinnaam/record (Host/Prt/A/CNAM/MX)	10	
Opheffen	Opheffen DNS domeinnaam/record (Host/Prt/A/CNAM/MX)	10	
Wijzigen	Wijzigen DNS domeinnaam/record (Host/Prt/A/CNAM/MX)	5	
DDI – Gedelegeerd beheer			
Aanvragen	Aanvragen DNS/DHCP/IPAM gedelegeerd beheer groep	10	
Opheffen	Opheffen DNS/DHCP/IPAM gedelegeerd beheer groep	10	
Wijzigen	Wijzigen DNS/DHCP/IPAM gedelegeerd beheer groep	10	
DDI – IPAM			
Aanvragen	Aanvragen/opvoeren van een (nieuw) netwerk, of nieuwe eigenaren van bestaand netwerk	10	
Opheffen	Opheffen van netwerk informatie van netwerken binnen een VPN	10	
Wijzigen	Opvoeren/update van host informatie binnen een netwerk	5	
DMZ en DMZ Client			

VPN			
Aanvragen	Aanvragen DMZ	30	
Opheffen	Opheffen DMZ	10	
Aanvragen Client	Aanvragen Client aansluiting	20	
Opheffen Client	Opheffen Client aansluiting	10	
Wijzigen Client	Wijzigen Client aansluiting	5	
Forward Webproxy			
Aanvragen	Aanvragen Forward Webproxy	In overleg	
Opheffen	Opheffen Forward Webproxy	In overleg	
Wijzigen	Wijzigen Forward Webproxy	In overleg	
Mail Relay			
Aanvragen	Aanvragen Mail Relay	In overleg	
Opheffen	Opheffen Mail Relay	In overleg	
Wijzigen	Wijzigen Mail Relay	In overleg	

Tabel 4 Bestelbare items VPN diensten

Levering gebeurt door Quanza – O&A met uitzondering van de Standaard Service Requests, die door Quanza – IB worden uitgevoerd. Voor alle werkzaamheden op locatie wordt SPIE aangestuurd.

Categorie VPN aansluiting
De categorie Virtual Private Network (VPN) aansluiting beschrijft verschillende type aansluitingen: de **VPN aansluiting** (bedraad middels RWS glasverbindingen of huurlijnen), de **Draadloze VPN aansluiting** en de **VPN Aansluiting ten behoeve van derde partijen** (externe koppeling).

Beheren IT-netwerkdiensten (VPN-aansluitingen)
Quanza IB voert het beheer uit op deze VPN diensten conform onderstaande SLA.

Dienstenmatrix VPN Aansluiting										
Type VPN Aansluiting	Bandbreedte	Beschikbaarheid					Storingshersteltijd in 95% van de gevallen			
		Enkel	Dubbel**	Redundant	Ipsec	Ipsec MCPE	Service Window Kantoortijden			Service Window"24/7"
		99,50%	99,80%	99,99%	99,99%	98%				
		Onbeschikbaarheid per jaar								
		ca 1d20u	ca 17u30m	ca 0u52m	ca 0u52m	ca 7d7u	8 uur	4 uur	8 uur	4 uur
Bedraad ****	< 10Mb (128/256/384 /512/640/768 /896 Kbps) (1/1.25/1.5/1. 75/2/3/4/5/6/ 7/8/9 Mbps)	V	V	V						
	10 Mb tot 1 Gb (10/20/30/40/ 50/60/70/80/ 90/100/200/ 300/400/500/ 600/700/800/ 900 Mbps)	V	V	V				V		V
	!Gb tot en met 10Gb 91/2/3/4/5/6/ 7/8/9 Gbps)	V	V	V						
Draadloos	2G of 4G ***	V	V*							V
Externe koppeling	Geen garantie	V	V	V	V	V				
RKN		V		V			V			V

*	Beschikbaar als Ruggedized (Router geschikt voor ongeconditioneerde ruimte)
**	Variant wordt beperkt ingezet. Indien het niet mogelijk is dubbel te ontsluiten, dan is het mogelijk de enkele variant dubbel uit te voeren middels een mobiele backup. Voor de mobiele backup is beschikbaarheid niet gegarandeerd.
***	Afhankelijk van ingezette hardware, geen bandbreedte garantie.
****	Dit betreft een bruto bandbreedte van huurlijnen. De netto bandbreedte bestaat uit de bruto bandbreedte minus een eventuele tunneloverhead van max 8Kbps

Tabel 5 Dienstenmatrix categorie VPN - aansluiting

Bestelbare items en levertijd

Voor de VPN aansluiting gelden de in onderstaande tabel weergegeven bestelbare items en bijbehorende levertijden.

VPN Aansluiting			
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen (door SP-O&A)**	**SSR (door SP-IB)**
Bedraad			
Aanvragen	Leveren 1e VPN aansluiting (levering en installatie verbinding + apparatuur)	90	
Opheffen	Opheffen laatste VPN aansluiting (opheffen verbinding + verwijderen apparatuur)	10	
Activeren	Activeren nieuwe VPN aansluiting (op afstand) op bestaand apparaat waar al tenminste één andere VPN aansluiting is aangesloten.	5	
Deactiveren	Deactiveren VPN aansluiting (op afstand) waarna er nog minstens één VPN aansluiting op het apparaat overblijft.	5	
Toeslag Hub-Spoke	Toeslag voor het activeren of deactiveren van de Hub-Spoke functionaliteit op een VPN aansluiting	x	

VPN Aansluiting			
Wijzigen	Wijzigen optie instelling(en) bestaande VPN aansluiting (op afstand)	5	
Aanvragen back-up Mobiel	Leveren back-up Mobiel	20	
Opheffen back-up Mobiel	Opheffen back-up Mobiel	10	
VPN Aansluiting Connect en Inter Connect			
Activeren – LO Enkelvoudig (99,5%)	Activeren extra VPN aansluiting op afstand	In overleg	
Activeren – LO Redundant (99,99%)	Activeren extra VPN aansluiting op afstand	In overleg	
Deactiveren	Deactiveren extra VPN aansluiting op afstand	In overleg	
Wijzigen	Wijzigen instellingen bestaande VPN aansluiting op afstand	In overleg	
Draadloos			
Aanvragen	Leveren 1e VPN aansluiting op apparaat (met en zonder installatie(*))	90	
Opheffen	Opheffen draadloze VPN aansluiting (met en zonder installatie(*))	90	
Wijzigen	Wijzigen configuratie	5	
Activeren	Activeren extra VPN aansluiting op afstand	5	
Deactiveren	Deactiveren extra VPN aansluiting op afstand	5	
Wijzigen	Wijzigen instelling bestaande VPN aansluiting op afstand	10	
Aanvragen Dekkingsmeting Mobiel	Leveren dekkingsmeting mobiele ontvangst inclusief rapport	5	
Externe Koppeling			
Aanvragen IPsec	Leveren IPsec verbinding	10	
Opheffen	Opheffen IPsec verbinding	10	
Wijzigen	Wijzigen IPsec verbinding	5	Ja
Aanvragen MCPE	Leveren Managed CPE met apparaat Aanvragen beheerde router Verplicht bij externe koppeling op basis van vaste verbinding, optioneel bij IPsec	90	
Opheffen MCPE	Opheffen verbinding met en het opruimen van beheerde router	20	
Wijzigen MCPE	Het aanbrengen van wijzigingen in de routering in de MCPE(s)	10	
Aanvragen vaste verbinding(**)	Aanvragen ON2013 verbinding (i.c.m. MCPE)	90	
Opheffen vaste verbinding (**)	Opheffen ON2013 verbinding (i.c.m. MCPE)	10	

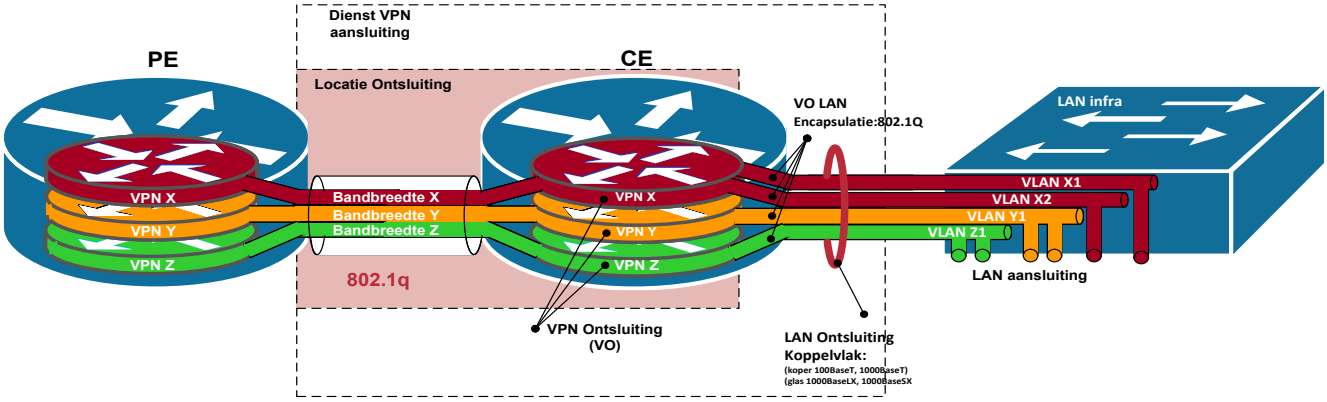
VPN Aansluiting			
RKN aansluiting			
Aanvragen	Van toepassing wanneer hardware geleverd moet worden of op een nieuw VPN moet worden aangesloten	90	
Activeren	Activeren extra VPN aansluiting op afstand	5	
Wijzigen	Wijzigen instelling bestaande VPN aansluiting op afstand	5	
Deactiveren	Deactiveren VPN aansluiting op afstand	5	
Opheffen	Van toepassing wanneer hardware gede-installeerd moet worden of wanneer door opzegging van de laatste aansluiting tevens een VPN moet worden gedeactiveerd	10	

Tabel 6 Bestelbare items categorie VPN aansluiting

Levering gebeurt door Quanza – O&A met uitzondering van de Standaard Service Requests, die door Quanza – IB worden uitgevoerd. Voor alle werkzaamheden op locatie wordt SPIE aangestuurd.

VPN aansluiting Bedraad

De VPN aansluiting omvat de fysieke en logische koppeling van een VPN met de LAN infrastructuur op een RWS -of RWS klantlocatie zoals schematisch is weergegeven in Figuur 2.



Figuur 2 Schematische weergave van de VPN aansluiting

De VPN aansluiting dient als ontsluiting tussen de RWS backbone en de LAN infrastructuur waarop eindsystemen zijn aangesloten. Op dezelfde hardware en transmissie kunnen meerdere VPN aansluitingen geleverd worden. Deze VPN aansluitingen zijn een logisch component op de fysieke hardware.

De VPN aansluiting is de aansluiting middels fysieke transmissie (RWS glas, huurlijnen of Dark Fiber Derden*) en biedt de volgende functies en opties ten behoeve van de LAN infrastructuur op een RWS of RWS klant locatie:

- Toegang tot een bestaand VPN;
- 100MB(UTP), 1GE (UTP of Glas) of 10GE (Glas) fysiek koppelvlak naar LAN infrastructuur;
- DHCP relay functionaliteit ten behoeve van DHCP;

- Wake on LAN;
- Eén of meerdere VLAN's, met per VLAN een IPv4 gateway adres en eventueel routering.

* Inzet van een Dark Fiber van andere (overheids-) partijen door RWS is in uitzonderlijke gevallen mogelijk wanneer Eigen Glas niet beschikbaar is. Hiervoor is expliciete goedkeuring van de domeineigenaar van Infra Netwerken nodig en is uitsluitend te bestellen door medewerkers van CIV IRN Infra Netwerken.

Functies en opties VPN aansluiting

De verschillende functies en opties voor de VPN aansluiting zijn hieronder beschreven.

A. VPN aansluiting type hub of type spoke

Wanneer er een nieuw VPN besteld wordt, kan men de keuze maken voor een any-to-any of een Hub-Spoke-VPN. Wanneer gekozen is voor een VPN type Hub-Spoke zal er per locatie aangegeven moeten worden bij de VPN aansluitingen of dit een Hub of een Spoke locatie betreft. Bovendien zal voor dit type VPN aansluiting per locatie tevens de activiteit toevoegen Firewall rule moeten worden besteld.

- VPN Aansluiting Type Spoke; Spokes zijn decentrale knooppunten die verbonden zijn met maximaal één Hub. Spokes kunnen niet onderling communiceren, alleen via de hub.
- VPN Aansluiting Type Hub; de Hub is het belangrijkste knooppunt in het Hub-Spoke netwerk. Het dient als centrale punt voor het beheer, de controle en de distributie van gegevens. En heeft meer bandbreedte dan de Spokes. De Hub-locaties worden beperkt tot de Centrale Voorzieningen, Verkeerscentrales en ODC locaties.

De VPN Aansluitingen type Hub en Spoke zijn met een gelijke beschikbaarheid te bestellen als een standaard VPN Aansluiting (enkel 99,5%, dubbel 99,8%, redundant 99,99%).

B. Bandbreedte

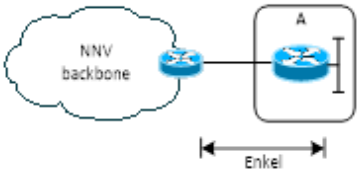
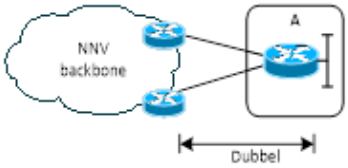
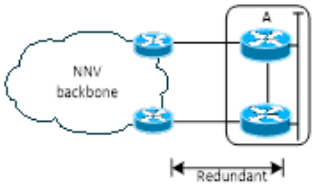
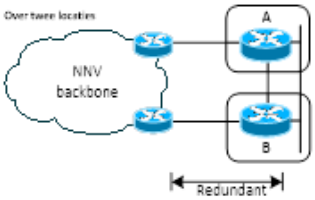
Op een Router/CE worden naast de Klant-VPN's maximaal 3 Beheer-VPN's geconfigureerd:
- Ten behoeve van de Router [CE:MGT]
- Ten behoeve van KA LAN Switch(es) [LAN:MGT]
- Ten behoeve van Overige LAN Switch(es) [EXT:MGT]

De bandbreedte voor een Beheer-VPN is afhankelijk van de bandbreedte van de VPN Ontsluiting:
- 128Kb voor 2Mb en 10Mb
- 1Mb voor 100Mb
- 10Mb voor 500Mb, 1Gb en 10Gb

De bandbreedte optie komt daadwerkelijk overeen met de geconfigureerde bandbreedte (in geval dat shaping mogelijk is).
Er wordt niet overboekt. Dat betekent dat de optelsom van de Klant-VPN's en Beheer-VPN's bandbreedtes samen kleiner of gelijk aan de bandbreedte van de VPN ontsluiting moet zijn (geldig voor zowel RWS Glas als ontsluiting middels huurlijn).

C. Beschikbaarheid

De VPN Aansluiting heeft vier beschikbaarheidsopties waarvan er drie zijn weergegeven in Figuur 3. De beschikbaarheid op locatie wordt bepaald door de VPN Aansluiting met de hoogste beschikbaarheidseis. Een beschikbaarheid van 99,999% kan uitsluitend worden aangevraagd via RWS CIV IRN Infra Netwerken als maatwerk.

Beschikbaarheid VPN Aansluiting		
Enkel	**Dubbel**	**Redundant**
99,5% 	99,8% 	99,99%  99,99% 
middels één tracé ontsloten naar één backbone router.	middels geografisch gescheiden tracés ontsloten naar twee geografisch gescheiden backbone routers.	

Figuur 3 Beschikbaarheid VPN Aansluiting

D. DHCP relay

Middels Dynamic Host Configuration Protocol (DHCP) kunnen eindsystemen binnen een LAN segment (VLAN) dynamisch van IP adressen worden voorzien. Met de DHCP relay functie kunnen per LAN segment de hiertoe toegewezen DHCP servers worden ingesteld. Er wordt een maximum van 3 DHCP servers per LAN segment ondersteund.

E. WoL

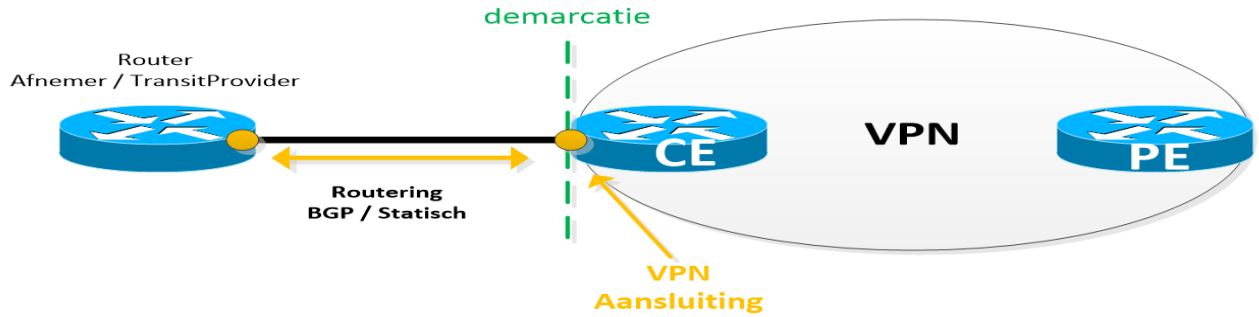
Wake on LAN (WoL) biedt de mogelijkheid netwerk devices op afstand te starten, bijvoorbeeld voor onderhouds- werkzaamheden.

F. Routering

Door middel van een LAN ontsluiting wordt een fysieke koppeling met de LAN infrastructuur tot stand gebracht. Deze wordt geleverd als een laag 3 interface. Elk LAN domein wordt op een gescheiden CE domein gekoppeld met een unieke LAN Ontsluiting.
In de dienstverlening worden vier routeringsopties onderscheiden: standaard, statisch, dynamisch type “Connect” en dynamisch type “InterConnect”. Deze worden hieronder nader toegelicht.

1. Standaard routering

Standaard wordt routering ingericht doormiddel van een VLAN-interface op de LAN aansluiting (VPN Ontsluiting LAN) zoals weergegeven in Figuur 4. Er kunnen meerdere VPN Ontsluiting (VO) LANs per VPN Aansluiting worden ingericht. De VPN Aansluiting is beperkt tot een enkel LAN domein.

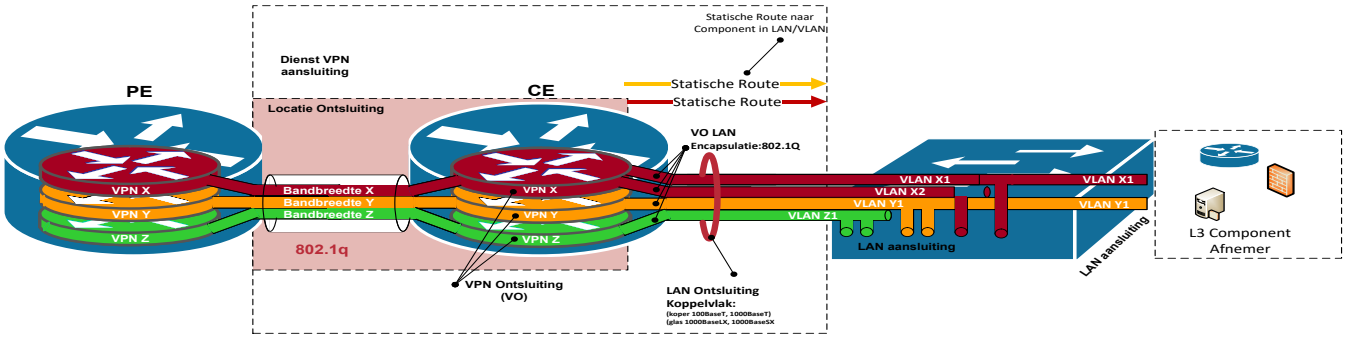


Figuur 4 Standaard routering VPN Aansluiting

Afwijkend kan routering naar een Laag 3 component op het Local Area Network (LAN) van de VPN-Aansluiting ingericht worden. Deze routering kan naar keuze statisch of dynamisch geleverd worden.

2. Statische routering

Indien gewenst is het ook mogelijk routering naar een component achter de VPN Aansluiting toe te passen doormiddel van statische routering zoals weergegeven in onderstaand figuur. Deze optie maakt het mogelijk om een component op het LAN aan te sluiten om zo een extern netwerk te kunnen benaderen. Het is niet toegestaan om tussen RWS netwerken te routeren.

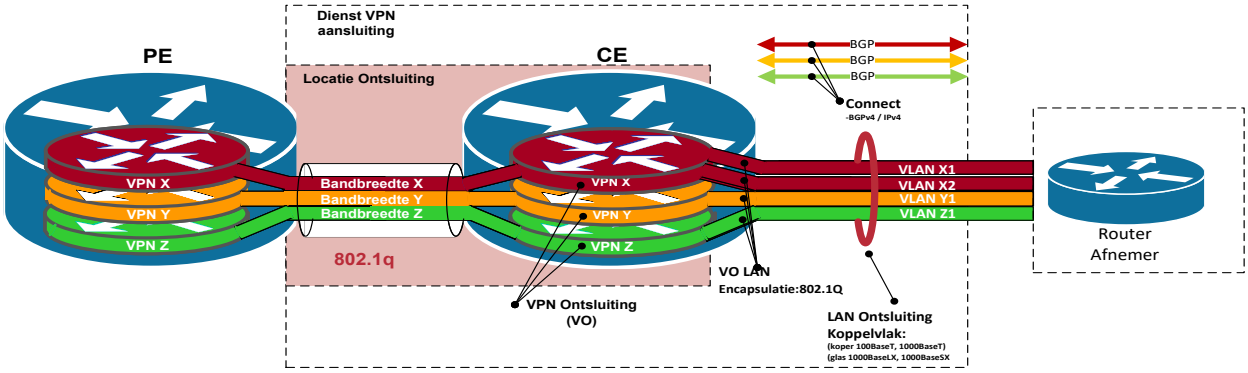


Figuur 5 Statische routering VPN Aansluiting

Voor meer informatie omtrent deze optie kan contact opgenomen worden met Service Management.

3. Dynamisch: VPN Aansluiting Connect

De VPN Aansluiting Connect, zoals weergegeven in onderstaand figuur, maakt het middels dynamische routering mogelijk netwerk-informatie uit te wisselen tussen het VPN en de afnemer. Deze optie is beschikbaar voor afnemers die geen transit-functionaliteit vervullen.



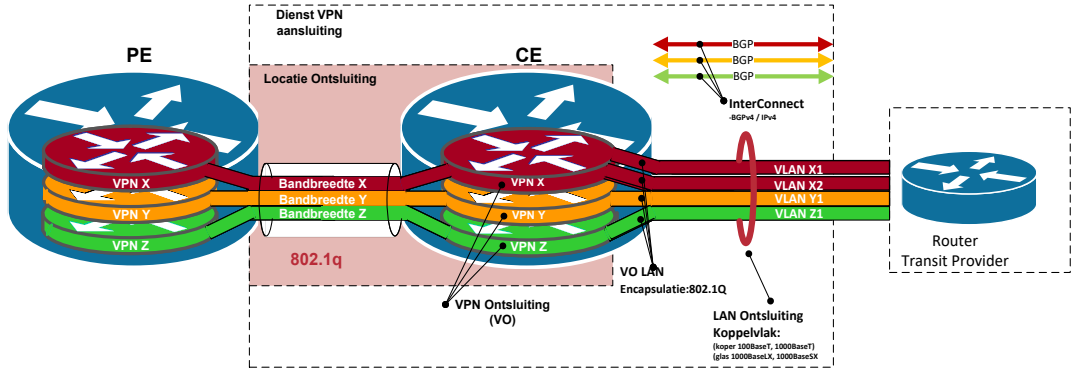
Figuur 6 Dynamische routering - VPN Aansluiting Connect

Voor een VPN-Aansluiting Connect op basis van dynamische routering zijn onderstaande uitgangspunten van toepassing:

- Klantapparatuur wordt direct op de LAN Ontsluiting aangesloten;
- Er wordt gebruik gemaakt van BGPv4. Hiermee is deze optie beperkt tot IPv4;
- Per VPN Aansluiting wordt één BGP-sessie toegestaan;
- Bij een redundante Locatie Ontsluiting is een redundante BGP koppeling mogelijk, waarbij één van de koppelingen als primair wordt behandeld en de tweede als secundair (back-up). De afgenomen bandbreedte geldt voor de gehele redundante koppeling;
- Toepassing van de BGP Attributen AS-Path prepending en MED wordt ondersteund;
- Standaard adverteert de VPN Aansluiting de gehele routeringstabel van het VPN. Optioneel is het mogelijk om een default-route toe te voegen of enkel een default route te adverteren naar de transit-provider;
- De afnemer van de VPN Aansluiting dient gebruik te maken van een Publieke AS. Indien de afnemer hier niet over beschikt wijst de Service Provider van RWS CIV IRN Infra Netwerken een Private AS toe;
- De afnemer mag niet als 'transit' fungeren voor andere partijen;
- Standaard worden max. 100 IPv4 routes van de afnemer geaccepteerd. In overleg kan dit worden aangepast;
- De afnemer van de VPN Aansluiting geeft de IP-netwerken op die worden geadverteerd naar de VPN Aansluiting. De Afnemer kan een ruimer IP-subnet opgeven en daarbinnen kleinere IP-netwerken adverteren (Bijvoorbeeld 172.16.0.0/16 opgeven waarbinnen enkel 172.16.1.0/24 en 172.16.2.0/24 worden geadverteerd door de Afnemer naar RWS);
- De IP-netwerken van de afnemer moeten conformeren aan het IP-plan van het VPN;
- Multicast wordt niet ondersteund.

4. Dynamisch: VPN aansluiting InterConnect

De VPN aansluiting InterConnect, zoals weergegeven in onderstaand figuur, is een optie op de VPN aansluiting om middels dynamische routering netwerk-informatie uit te wisselen met het VPN en wordt gebruikt om het RWS netwerk te koppelen met andere transit/provider netwerken.



Figuur 7 Dynamische routering - VPN Aansluiting InterConnect

De VPN-Aansluiting InterConnect koppelt een VPN op het domein van RWS met een VPN op het domein van de transit-provider. Route uitwisseling vindt plaats middels BGPv4.

De volgende uitgangspunten zijn van toepassing:

- Apparatuur van de transit-provider wordt direct op de LAN Ontsluiting aangesloten;
- Er wordt gebruikgemaakt van BGPv4. Hiermee is deze optie beperkt tot IPv4;
- Per VPN aansluiting wordt één BGP-sessie toegestaan.
- Bij een redundante Locatie Ontsluiting is een redundante BGP koppeling mogelijk, waarbij één van de koppelingen als primair wordt behandeld en de tweede als secundair (back-up). De afgenomen bandbreedte geldt voor de gehele redundante koppeling;
- Toepassing van de BGP Attributen AS-Path prepending en MED wordt ondersteund;
- Standaard adverteert de VPN Aansluiting de gehele routeringstabel van het VPN. Optioneel is het mogelijk om een default-route toe te voegen of enkel een default route te adverteren naar de transit-provider;
- De VPN-aansluiting fungeert als transitkoppeling. Het BGP AS-plan wordt in overleg afgestemd;
- Publieke BGP AS-nummers worden standaard geaccepteerd. Gebruik van Private AS-nummers
- worden vooraf afgestemd;
- Standaard worden maximaal 1000 IPv4-routes per VPN geaccepteerd vanuit de transit-provider. In overleg kan deze waarde verhoogd worden;
- De IP-netwerken die door de transit-partij worden geadverteerd maar RWS dienen aan het IP-plan van het VPN te voldoen;
- Multicast wordt niet ondersteund.

VPN aansluiting type RKN (Rijkswaterstaat Koppel netwerk)

Rijksoverheden en Overheden maken gebruik van verschillende Wide Area Netwerken met als doel een communicatie-infrastructuur te realiseren. Optimale samenwerking tussen alle

(Rijks)overheids-partijen is cruciaal, waarbij overdracht en gebruik van informatie tussen partijen een belangrijk uitgangspunt is.

Het Rijkswaterstaat Koppel Netwerk (RKN) is aangesloten op het centrale Koppelnet Publieke Sector (KPS) en biedt en ontsluiting naar koppelnetwerken van andere (Rijks)overheidspartijen op basis van het Diginetwerk Afsprakenstelsel. Tevens biedt RKN ontsluiting naar het koppelnet van DMO RON2.0 (WAN-I, DCI, Rijksweb en DWR).

Partners van RWS kunnen met de bouwsteen Rijkswaterstaat Koppel Netwerk (RKN) als "aangesloten overheidsorganisatie" aangesloten worden op het Rijkswaterstaat Koppel Netwerk (RKN) en transit aanvragen naar (een) andere aangesloten overheidsorganisatie(s).

De bouwsteen Rijkswaterstaat Koppel Netwerk (RKN) is een integratie-dienst, waarbij de bouwsteen 'VPN' en de bouwsteen 'VPN aansluiting' worden samengevoegd. Alle service management communicatie (eenmalige diensten, incidenten, rapportages, capaciteitsmanagement etc.) vindt plaats o.b.v. de RKN-bouwsteen.

Nieuwe transit providers kunnen via de Service Manager worden toegevoegd op basis van RFI (conform het SPM-proces) en nieuwe transit VPN's kunnen worden aangevraagd op basis van de PDC dienst RKN.

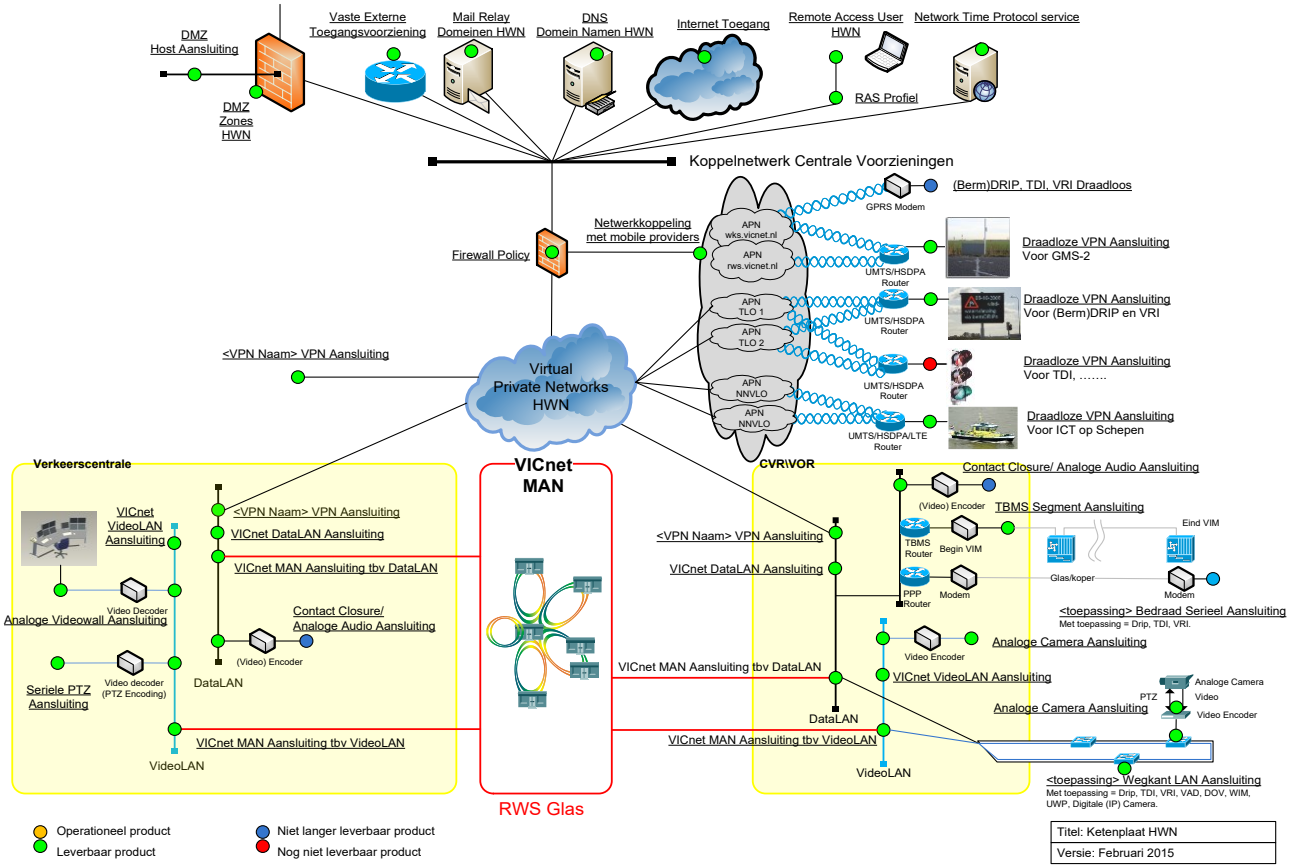
Voor de afnemers van diensten over het RKN-netwerk wordt een VPN aansluiting. Enkelvoudig gerealiseerd op één RWS ODC-locatie of een VPN Aansluiting Redundant over de RWS ODC-locaties AM2/AM3. Per afnemer wordt per RWS ODC-locatie één fysieke interface beschikbaar gesteld welke meerdere logische VPN-aansluitingen kan leveren.

De oplossing voorziet in statische of dynamische routering aan de kant van de afnemers. De verantwoordelijkheid van SP-O&A eindigt op de patchpanelen waarop de apparatuur van RWS is afgewerkt.

Maandelijkse rapportage op incident, problem, availability, capacity en changes per deelnemer per koppeling aan de SLM van RWS. Naast een klantrapportage wordt ook een totaalrapportage op de interface aan de providerkant voor capacity management geleverd.

VPN aansluiting type Draadloos

De draadloze VPN aansluiting is de mobiele en logische koppeling van een VPN met de LAN infrastructuur op een RWS -of RWS klantlocatie zoals schematisch is weergegeven in Figuur 8 en is inzetbaar om zowel locaties als apparaten aan te sluiten. De aansluiting bestaat uit een draadloze router voorzien van mobiele SIM-kaart(en).



Figuur 8 Schematische weergave draadloze VPN Aansluiting

De Draadloze VPN aansluiting biedt dezelfde functionaliteiten als de VPN aansluiting zoals beschreven in bovenstaande paragraaf met afwijkende beschikbaarheid. De Draadloze VPN aansluiting is niet geschikt voor missiekritieke systemen. Door het gebruik van publieke draadloze infrastructuur kan niet aan BIV-normen worden voldaan. Bovendien is gebruik van Multicast niet toegestaan.

Aanvullend gelden de volgende functionaliteiten:

- Transmissie 2G/4G (op schepen wordt geen gebruik gemaakt van 2G transmissie);
- Single SIM voor standaard beschikbaarheid (legacy, niet bestelbaar) of Dualprovider/ Dual SIM voor hogere beschikbaarheid;

- In ongeconditioneerde omgevingen wordt een Ruggedized router geleverd. Langs de weg kant is dit verplicht.

De dienst kent de volgende eigenschappen:

- Simkaarten worden altijd meegeleverd met de beheerde router, andere Simkaarten mogen niet gebruikt worden;
- Afhankelijk van de dekkingsgraad van mobiel zijn er verschillende antenne opties beschikbaar;
- Afnemer kan ervoor kiezen de installatie door de RWS aannemer te laten uitvoeren;
- Voor inbouw in weg- of waterkanttoepassingen gelden veelal specifieke montagevoorschriften die beschikbaar zijn op de VPR.

SIM-kaarten
Bij een draadloze VPN aansluiting wordt de connectiviteit verzorgd met behulp van twee SIM-kaarten. In verband met de business continuity eisen is er een primaire en een secundaire SIM-kaart nodig bij twee verschillende mobiele providers. Onder het contract ON2013 zijn dit Vodafone (primair) en KPN (secundair). In het nieuwe contract CDR2023 zijn dit ODIDO (primair) en Vodafone (secundair).
(*) "Met installatie" betekent, dat de installatie door SPIE gebeurt; "zonder installatie" betekent, dat de SPIE de hardware voorbereidt tot en met staging, maar dat de installatie zelf door een lokale aannemer gebeurt.

VPN aansluiting type externe koppeling
De dienst Externe Koppeling maakt het mogelijk om een niet-RWS-netwerk op een vaste locatie veilig permanent te koppelen met het RWS-netwerk. Hiermee is permanente beveiligde transparante netwerkcommunicatie mogelijk.
Toepassingen hiervoor zijn bijvoorbeeld machine-to-machine communicatie zoals beheersystemen van derde partijen die directe en transparante koppeling tot de door hen beheerde systemen op het RWS-netwerk nodig hebben.
Afhankelijk van de gebruikte transporttechnologie en al dan niet toegepaste redundantie kunnen er SLA's gegeven worden op de beschikbaarheid van en bandbreedte voor deze communicatie.

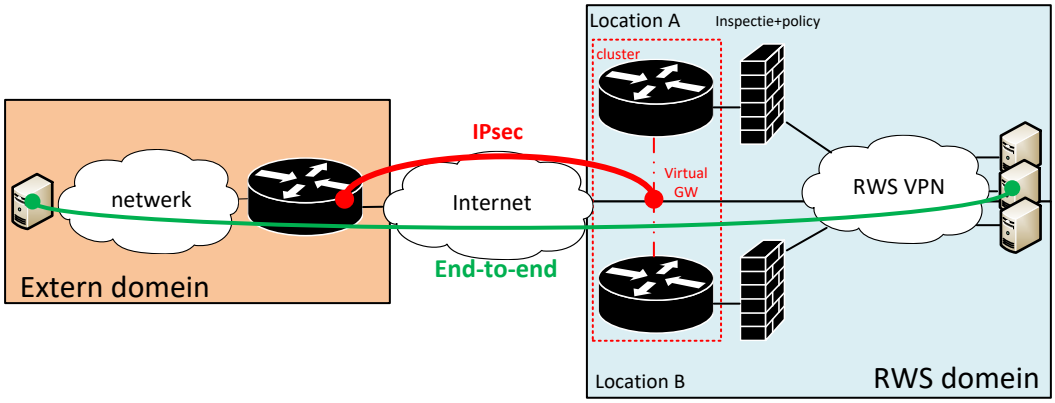
De Externe Koppeling maakt het mogelijk om via een (un)trusted netwerk (bv internet) veilig een niet RWS locatie te ontsluiten naar het RWS netwerk. De vertrouwelijkheid en integriteit van de data wordt gewaarborgd door gebruik te maken van een overlay techniek op basis van IPsec waarin de data versleuteld verstuurd wordt tussen RWS en de aangesloten partij. Er kan ook gekozen worden om een externe koppeling te realiseren via een vaste VPN aansluiting die wordt gekoppeld aan het RWS netwerk.

De externe partij kan er voor kiezen eigen apparatuur in te zetten die logisch wordt aangesloten op het RWS netwerk. Deze partij zal zich wel moeten conformeren aan de interfaces (Zie hfst 3) gesteld vanuit SP-O&A, hierbij moet gedacht worden aan de communicatie protocollen en encryptie standaarden om de data veilig te kunnen

transporteren. Deze interfaces kunnen van tijd tot tijd worden aangepast als er bv nieuwe standaarden zijn voor de gebruikte encryptiemethoden. Van de aangesloten partij mag worden verwacht dat deze mee gaat met deze nieuwe voorwaarden.

Op dit moment worden er drie opties geboden voor het leveren van een externe verbinding:

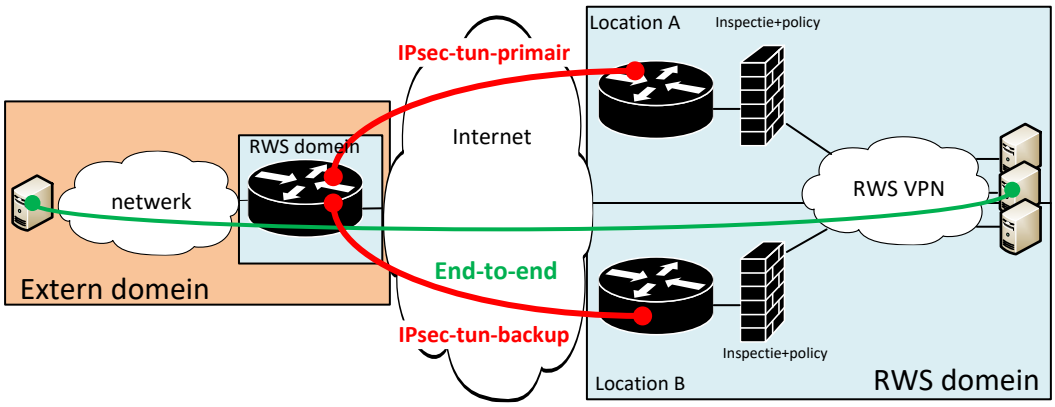
IPSEC zonder managed CPE
IPSEC zonder managed CPE is weergegeven in onderstaand figuur en redundant opgebouwd aan de RWS zijde waarbij de apparatuur over twee geografisch gescheiden locaties een cluster vormt. Op deze omgeving worden alleen nog de marktconforme veilige encryptie standaarden gebruikt. Er wordt gebruik gemaakt van een virtual IP adres voor de VPN gateway. Hierdoor is de perceptie van de afnemer dat er slechts één component staat.



Figuur 9 IPSEC

IPSEC met managed CPE (MCPE)
Bij deze optie, weergegeven in onderstaand figuur, wordt het internet gebruikt als transportmedium tussen het RWS netwerk en de externe partij. De externe partij dient zorg te dragen voor een werkende internet verbinding en een computerruimte waarin de apparatuur geïnstalleerd kan worden. Op locatie van de externe partij wordt een beheerd netwerk device geplaatst vanuit SP-O&A. SP O&A draagt zorg voor het opzetten van de veilige logische verbinding waarin het dataverkeer versleuteld wordt. Deze wordt aan de RWS-zijde redundant ontsloten over twee geografisch gescheiden locaties. SP-IB monitort actief de CPE die bij de externe partij staat.

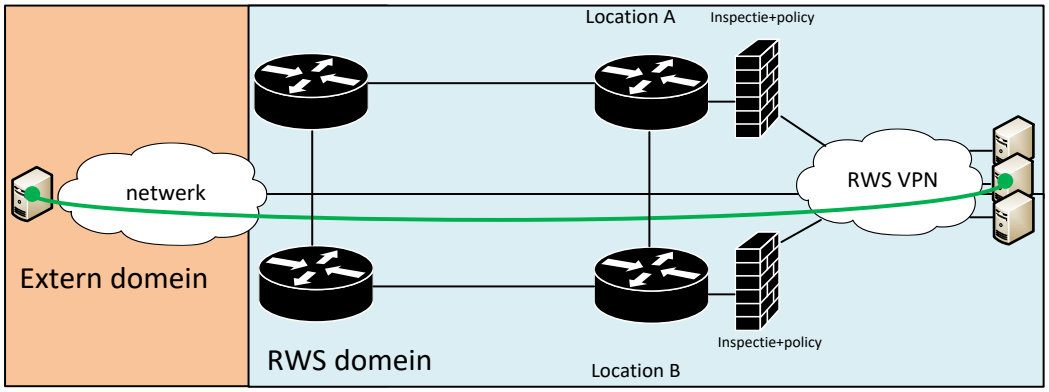
Voordelen	Nadelen
• Flexibel • Veilig • Relatief snel te leveren • Alleen een transparante internet verbinding nodig. • ConclusionQuanza zorgt voor een werkende end-to-end verbinding.	• End-to-end geen SLA af te geven • Geen bandbreedte garantie • Standaard alleen leverbaar binnen NL



Figuur 10 IPsec + MCPE

Vaste verbinding
Bij deze optie, weergegeven in onderstaand figuur, wordt een vaste verbinding ingezet vanuit de bouwsteen 'VPN aansluiting'. De VPN aansluiting zal op een veilige manier worden aangesloten op het RWS netwerk. De verbinding t/m de locatie van de afnemer valt onder de verantwoordelijkheid van ConclusionQuanza.

Voordelen	Nadelen
• Veilig • End-to-end SLA (zie SLA VPN aansluiting) • Diverse beschikbaarheid opties (zie VPN aansluiting) • Bandbreedte garantie	• Langere levertijd • Standaard alleen leverbaar binnen NL • Extra VPN + VPN Firewall nodig



Figuur 11 Voorbeeld redundante vaste verbinding

De dienst kent de volgende eigenschappen en uitgangspunten:

- Voor vaste externe toegangsvoorzieningen die geen SLA's vereisen wat betreft beschikbaarheid en bandbreedte, kan er gekozen worden om te koppelen via het internet en IPsec. De randvoorwaarde hiervoor is dat de niet-RWS-locatie beschikt over een eigen internetvoorziening met voldoende beschikbare netwerk capaciteit voor de beoogde communicatie.
- Apparatuur die op locatie bij een derde partij wordt geplaatst, dient te worden geplaatst in een ruimte die voldoet aan de eisen, beschreven in de NNV aansluitvoorwaarden.
- Voor beveiliging worden componenten gebruikt die aantoonbaar voldoen aan geaccepteerde beveiligingscriteria zoals NBV[1] goedkeuring of certificering volgens ISO/IEC 15408 (common criteria)[2] .
- De systeem eigenaar/ product manager van de beschikbaar gestelde applicaties, systemen, netwerken en informatie dient expliciet toestemming te geven voor deze netwerk toegang.
- De dienst is alleen voor CIV-onderdelen of externe partners die een contract afgesloten hebben met CIV. Voor het gebruik van de externe koppeling dienen externe partners te voldoen aan de “RWS-voorwaarden Externe koppelingen”.
- De klant conformeert zich bij afname van deze dienst expliciet aan het beveiligingsbeleid van Rijkswaterstaat.
- Iedere vaste externe toegangsvoorziening met een derde partij dient een benoemde functioneel beheerder te hebben.
- Vaste externe toegangsvoorzieningen worden bij voorkeur via het internet gerealiseerd via de standaard-beveiligingsfaciliteiten van NNV met gebruik maken van IPsec VPN-technologie.
- De vaste externe toegangsvoorziening voldoet aan de baseline beveiliging BIR2017.
- De vaste externe toegangsvoorziening ondersteunt alleen IPv4 unicast.
- Er kan alleen gebruik worden gemaakt van publieke adressen voor de communicatie tussen de externe partij en RWS.
- Routering tussen de externe partij en ConclusionQuanza is op basis van statische routes.

Bij het aanvragen of wijzigen van een vaste externe toegangsvoorziening voor een derde partij dient het “RWS Netwerktoegang voor Derden” proces gevolgd te worden. Dit proces kan opgestart worden door het invullen en bij de Corporate Servicedesk indienen van het “Aanvraagformulier Netwerktoegang voor Derden.”

Externe koppelingen in de vorm van vaste verbindingen
(**) Externe koppelingen in de vorm van vaste verbindingen worden afgenomen via het ON2013 contract; medio 2025 wordt dit vervangen door het CDR2023 contract. Leverancier is voor beide contracten ODIDO.

[1] NBV: Nationaal Bureau voor Verbindingsbeveiliging, onderdeel van het ministerie van BZK.
[2] Voor een common criteria beoordeling moet een bewuste keuze worden gedaan voor een EAL-niveau en een protection profile dat voldoende is voor de toepassing.

Het gaat om de volgende dienstverlening door ODIDO:

IP & Ethernet VPN	20Mb/s, Beheerprofiel Laag	BD01
	20Mb/s, Beheerprofiel Standaard	BD02
	20Mb/s, Beheerprofiel Hoog	BD03
	100Mb/s, Beheerprofiel Standaard	BD11
	100Mb/s, Beheerprofiel Hoog	BD12
	1Gb/s, Beheerprofiel Standaard	BD21
	1Gb/s, Beheerprofiel Hoog	BD22
	1Gb/s, Beheerprofiel Non-stop	BD23
On-Net maken, Odido	On-net maken (glasvezel), opstartkosten	AG01
	On-net maken (glasvezel), graafkosten per meter	AG02
	On-net maken (glasvezel), kosten boren per meter	AG03
	On-net maken (radioverbinding)	AG04
On-Net maken, Inkoop 3e partij	Opslag op eenmalig kosten bij inkoop 3de partij	TP01
	Opslag op maandelijkse kosten bij inkoop 3de partij	TP02
PSTN Verbindingen	PSTN (koper), Beheerprofiel Laag	PS01
	PSTN (glas), Beheerprofiel Laag	PS02
	PSTN (glas), Beheerprofiel Hoog	PS03

Tabel 7 Vaste verbindingen ODIDO

Categorie LAN aansluiting

Een LAN aansluiting maakt het mogelijk om op RWS locaties connecties te maken over het netwerk. De categorie **Local Area Network (LAN) aansluiting** omvat de verschillende type LAN aansluitingen voor Kantoor Automatisering-LAN (KA-LAN en LAN aansluiting type KA), WIFI, Centrale VicNet Ruimte (CVR) en VicNet Object Ruimte (VOR), Wegkant/Waterkant systemen, Gebouwen, Rekencentrum (VC/VP) en type Offshore voor aansluitingen op zee.

Functionele omschrijving

De dienst LAN aansluiting biedt toegang tot een virtueel netwerk via een fysieke LAN poort. De LAN aansluiting is opgebouwd uit de volgende componenten:

LAN ontsluiting dit is de logische koppeling naar een specifiek VPN
VLAN dit is een virtueel LAN (VLAN) in de fysieke infrastructuur (bijvoorbeeld de switches)
LAN aansluiting de fysieke poort die toegang biedt naar het virtuele LAN
Network Access Control (NAC) Netwerktoegangsbeveiliging op LAN niveau. Eindgebruikers en eindsystemen krijgen pas netwerktoegang na succesvolle authenticatie.

Ethernet infra dit is de fysieke infrastructuur (bekabeling en switches)

Ethernet Infra
Het component Ethernet infra is zo opgebouwd dat de dienst LAN aansluiting bijna overal leverbaar is. Hiervoor moet wel bekabeling aanwezig zijn, of aan te leggen zijn, tegen acceptabele kosten. Deze dienst biedt een fysieke ethernet aansluiting voor een eindsysteem. Deze wordt op een door een VPN ontsloten locatie gerealiseerd middels een VPN aansluiting.

Network Access Control (NAC)
Wanneer een eindgebruiker of eindsysteem verbinding maakt met het netwerk wordt met behulp van NAC (Network Access Control) bepaald of deze geautoriseerd is om toegang tot het netwerk te hebben. Door middel van NAC wordt ook bepaald tot welke gebruikersgroep de eindgebruiker behoort. De gebruikersgroepen worden vastgelegd in zogenaamde NAC-profielen (Informatie hierover is te vinden in paragraaf 0). NAC wordt verplicht ingeschakeld op LAN dienstverlening op kantoorlocaties. Hiervan kan alleen worden afgeweken bij devices die geen 801.2x ondersteunen. Een security exceptie is hiervoor randvoorwaardelijk. Deze zal door de afnemer zelf moeten worden aangevraagd binnen RWS.
NAC is generiek ontwikkeld, ook voor alle overige type LAN aansluitingen behalve op ODC LAN of op LAN aansluitingen die geïntegreerd zijn in een Backbone Edge(CE-router). Om NAC te gebruiken is een NAC profiel noodzakelijk. De Infra Adviseur Netwerken begeleidt het aanvragen van een profiel.

Beheren LAN-aansluitingen
RWS onderkent de volgende LAN-aansluitingen:
1. Gebouw
2. LAN-aansluiting type KA
3. Rekencentrum
4. CVR/VOR
5. Callcenter
6. Wegkant/Waterkant
7. Offshore
8. Wifi
9. Open Wifi

Quanza IB voert het beheer uit op deze LAN-diensten conform onderstaande SLA.

Dienstenmatrix LAN											
Type LAN Aansluiting	Bandbreedte	Beschikbaarheid						Storingshersteltijd in 95% van de gevallen			
		Enkel			Redundant			Service Window Kantoortijden		Service Window"24/7"	
		99,00%	99,50%	>99,7%	>99,8% **	99,95% ***	99,99% ***				
		Onbeschikbaarheid per jaar									
		ca 3d15u	ca 1d20u	ca 1d2u	ca 17u30m	ca 4u28m	ca 0u52m	8 uur	4 uur	8 uur	4 uur
Gebouw			V			V			V		V
Rekencentrum (VC/VP)			V			V			V		V
CVR/VDR	Auto (voorkeursinstelling)		V				V				V
	10 Mbps		V				V				V
	100 Mbps		V				V				V
	1000 Mbps		V				V				V
Callcenter	<= 100 Mbps of		V			V					V
	<= 1 GBps of		V			V					V
	<= 2 * 1 Gbps (Server)		V			V					V
Wegkant/Waterkant*	<= 1Gbps			V	V						V
KA LAN	<= 100 Mbps of		V			V		V	V		V
	<= 1 GBps of		V			V		V	V		V
	<= 2 * 1 Gbps (Server/blade)		V			V		V	V		V
Wifi****			V					V			

*	max 2 storingen per jaar
**	indien sprake is van geografische redundantie glasvezelinfrastructuur
***	over 2 switches
****	radiodekking
*****	type Offshore is Redelijke Inspanning (ivm specfieke locatie)

Tabel 8 Beschikbaarheids eisen LAN aansluiting

Bestelbare items levertijd

Voor de LAN aansluiting gelden de in onderstaande tabel weergegeven bestelbare items met bijbehorende standaard levertijden.

LAN Aansluiting			
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen (door SP-O&A)**	**SSR (door SP-IB)**
RWS Netwerk LAN *(Gebouw, Rekencentrum (VC/VP), CVR/VOR, KA)*			
Aanvragen	Leveren 1e LAN aansluiting op apparaat	60	
Opheffen	Opheffen laatste LAN aansluiting op apparaat	10	
Activeren	Activeren extra LAN aansluiting op afstand	5	
Deactiveren	Deactiveren extra LAN aansluiting op afstand	5	
Wijzigen	Wijzigen instelling bestaande LAN aansluiting op afstand (alleen voor LAN aansluiting KA)	5	
Wegkant/Waterkant, Onderstation, Offshore			
Aanvragen	Leveren 1e LAN aansluiting op apparaat	60	
Aanvragen	Leveren 1e LAN aansluiting op apparaat zonder installatie(*)	60	
Opheffen	Opheffen laatste LAN aansluiting op apparaat	10	
Opheffen	Opheffen laatste LAN aansluiting op apparaat zonder installatie(*)	10	
Activeren	Activeren extra LAN aansluiting op afstand	5	
Deactiveren	Deactiveren extra LAN aansluiting op afstand	5	
WIFI			
Aanvragen	Leveren access point	50	
Opheffen	Opheffen access point	20	
Wijzigen	Wijzigen instelling access point op afstand	5	

LAN Aansluiting			
Aanvragen site survey (per etage)	Leveren site survey op locatie	15	
Open WIFI			
Activeren Open WIFI	Open WIFI functionaliteit op locatie / verdieping / ruimte (excl. site survey) met of zonder apart SSID	20	
Deactiveren Open WIFI	Open WIFI functionaliteit op locatie / verdieping / ruimte (excl. site survey) met of zonder apart SSID	20	
Wijzigen Open WIFI	Registratie MAC adres vaste apparatuur per 10 devices	1	
Aanvragen site survey (per etage)	Leveren site survey Open WIFI op locatie	15	

Tabel 9 Bestelbare items categorie LAN aansluiting

Levering gebeurt door Quanza – O&A met uitzondering van de Standaard Service Requests, die door Quanza – IB worden uitgevoerd. Voor alle werkzaamheden op locatie wordt SPIE aangestuurd.

(*) Met installatie betekent, dat de installatie door SPIE gebeurt; zonder installatie betekent, dat de hardware wordt afgeleverd door SPIE, maar dat de installatie zelf door een lokale aannemer gebeurt.

RWS Netwerk LAN

Onder RWS Netwerk LAN worden alle LAN aansluitingen verstaan met uitzondering van Kantoor Automatisering LAN, WIFI en OpenWIFI. Deze specifieke diensten met bijbehorende kenmerken zijn separaat beschreven.

Op basis van de gewenste beschikbaarheid, bandbreedte, robuustheid en functionaliteit zijn er meerdere RWS Netwerk LAN opties mogelijk.

LAN aansluiting type Gebouw: *voor systemen met middelhoge snelheden en data throughput*

Dit type LAN aansluiting wordt toegepast voor systemen (onder andere datacollectie-pc's) met middelhoge snelheden en data throughput in RWS gebouwen zoals Industriële Automatisering (IA's) en Object LAN's. De uitvoering is op basis van een RJ45 koppelvlak. Redundante aansluiting van eindsystemen en loadbalancing zijn niet mogelijk.

LAN aansluiting type Rekencentrum (VC/VP): *voor systemen met hoge eisen aan beschikbaarheid en bandbreedte ten behoeve van Verkeerscentrales en Verkeersposten*

Dit type LAN aansluiting wordt ingezet voor systemen met hoge eisen aan beschikbaarheid en bandbreedte, toegepast in Verkeerscentrales en Verkeersposten. Uitvoering is op basis van een koper (RJ45) of glas-koppelvlak. Schaalbaarheid is in dit type LAN aansluiting mogelijk.

LAN aansluiting type CVR / VOR*: o.b.v. schaalbaarheid, robuustheid en hoge beschikbaarheid*

Dit type LAN aansluiting is bedoeld om in CVR/VOR ruimten langs Rijks(water)wegen een connectie te maken met verkeersmanagementsystemen in Verkeerscentrales (VC) en het RWS Overheid Data Center (ODC). De dienst biedt de noodzakelijke LAN functionaliteit ten behoeve van het aansluiten van inwin- en besturingssystemen zoals meetsystemen, camera's, radarsystemen, noodsystemen en signaleringsystemen. Belangrijke kenmerken zijn schaalbaarheid, robuustheid en hoge beschikbaarheid. Redundante aansluiting van eindsystemen en loadbalancing zijn niet mogelijk.

De volgende voorwaarden gelden voor het type LAN aansluiting CVR/VOR:

- Een geconditioneerde omgeving;
- De LAN aansluiting is uitsluitend bedoeld voor eindsystemen. Het aansluiten van netwerk apparatuur zoals routers, switches en access points op een LAN aansluiting is niet toegestaan;
- Deze dienst biedt uitsluitend ondersteuning voor TCP/IP en Ethernet. Andere protocollen zoals IPX/SPX of veldbus protocollen zoals Profinet, Modbus en SafetyNET worden niet ondersteund.
- Voor het aansluiten van digitale eind devices kan dit type LAN-aansluiting geleverd worden met optische SFP's (single of dual fiber). Aangesloten eind devices dienen in de directe omgeving van de switch te staan. Het demarcatiepunt van de dienstverlening op deze LAN aansluiting is de LAN-poort. Bekabeling vanaf de LAN-poort naar het eind device, en eventuele media convertor, zijn geen onderdeel van de dienst. Deze LAN poorten zijn expliciet alleen voor eind devices bedoeld zijn en niet om routers of switches aan te sluiten.

De duplex instelling van een LAN aansluiting wordt standaard ingesteld op de voorkeursinstelling (Auto) waarbij een onderhandelprotocol zorgt dat beide aangesloten apparaten dezelfde duplex instelling hebben. Hierbij wordt onderscheid gemaakt tussen Half Duplex (eenrichtingsverkeer, om en om zenden en ontvangen) en Full Duplex (tweerichtingsverkeer, tegelijk van beide kanten zenden en ontvangen mogelijk). Indien de Auto instelling voor beide aangesloten apparaten niet naar behoren werkt kan de aansluiting in sommige gevallen op Half of Full Duplex worden ingesteld.

LAN aansluiting type Wegkant/Waterkant *ten behoeve van ongeconditioneerde ruimtes*

Deze LAN aansluiting is bedoeld om ethernet/IP gebaseerde weg- en waterkant toepassingen te koppelen op een VPN. Deze dienst wordt onder andere toegepast bij DRIPs, DOV, TDI, VRI, VAD, Weigh In Motion weegbruggen (WIM), IP-camera's, Digitale Camera aansluitingen en het UWP. Het biedt een hoge beschikbaarheid en betrouwbaarheid waarbij het mogelijk is om onderdelen eenvoudig te vervangen met behoud van functionaliteit.

Afwijkend ten opzichte van andere ethernet/IP gebaseerde LAN producten worden omwille van de relatief grote afstanden de ethernetswitches in cascade (ring-topologie) geschakeld. Standaard is de beschikbaarheid redundant (>99,8%) door een geografisch gescheiden Glasvezelring (loopt via een geheel andere [vaar]weg dan wel aan de andere zijde van de [vaar]weg retour). Indien er geen geografisch gescheiden Glasvezelring mogelijk is, maar wel een fysieke Glasvezelring, kan op verzoek van de Afnemer en met toestemming van CIV Infra deze Dienst geleverd worden met een beschikbaarheid enkelvoudig (>99,7%; loopt via dezelfde [vaar]weg of via dezelfde Glasvezelkabel retour).
Deze dienst is geschikt gemaakt voor het leveren in ongeconditioneerde ruimtes doormiddel van passieve koeling en biedt ten behoeve van de service provider SP-IB remote beheerfunctionaliteit van de apparatuur voor netwerkmanagement.
In het kader van beveiliging worden niet gebruikte poorten dichtgezet, applicatiedomeinen in aparte VLAN's ondergebracht ten behoeve van de scheiding van netwerk services, switches in afgesloten kasten geplaatst, MAC Address filtering toegepast op wegkantswitches, vindt beheeradmin toegang plaats via de centrale AAA Service, is beheer van VLAN/VPN gescheiden van data VLAN's en wordt gebruik gemaakt van Detect en Disable unidirectional links.

Voor dit type LAN aansluiting geldt een aantal aanvullende voorwaarden:

- Plaatsing en montage op DIN rail, 19" rack of 'board' vereist;
- Er worden maximaal 27 switches cascade geschakeld;
- Met een 1000Base-LX interface kan een afstand worden bereikt van 10km en met de ZX variant ca 70km (conform specificaties) per switch;
- Voor het aansluiten van digitale eind devices kan dit type LAN-aansluiting geleverd worden met optische SFP's (single of dual fiber). Aangesloten eind devices dienen in de directe omgeving van de switch te staan. Het demarcatiepunt van de dienstverlening op deze LAN aansluiting is de LAN-poort. Bekabeling vanaf de LAN-poort naar het eind device, en eventuele media convertor, zijn geen onderdeel van de dienst. Deze LAN poorten zijn expliciet alleen voor eind devices bedoeld zijn en niet om routers of switches aan te sluiten.
- Deze LAN aansluiting wordt standaard geleverd met een dubbele (net)voeding. Indien noodzakelijk kan deze geleverd worden met een enkelvoudige voeding en/of een voeding met lage inschakelstroom (≤ 16 A). Bij gebruik van een enkelvoudige voeding wordt de beschikbaarheid naar 99,5% teruggebracht.

LAN aansluiting type Onderstation *ten behoeve van ongeconditioneerde ruimtes*

Deze LAN aansluiting is toepasbaar met en zonder WKS, en is geschikt om bijvoorbeeld camera's, DRIP's, TDI's, WIM's etc. op afstand van een WKS of CVR/VOR aan te kunnen sluiten. De LAN aansluiting type Onderstation wordt geleverd middels een switch met maximaal 4 aansluitmogelijkheden, met een enkelvoudige voeding en wordt enkelvoudig aangesloten via RWS glas. Hierdoor kent deze dienst een lagere beschikbaarheid garantie; maximaal 95%.

LAN aansluiting type Offshore

De dienst LAN aansluiting type Offshore biedt LAN aansluitingen op offshore objecten op de Noordzee, zoals Windmolenparken (WMP's), windturbinegeneratoren (WTG's) en olie-&gasplatforms. Deze dienst kent geen service levels, omdat er op zee geen garantie mogelijk is voor het tijdig beschikbaar hebben van apparatuur en monteurs. Vervangende hardware voor de LAN Aansluiting type Offshore is in geval van defecten binnen 24 uur beschikbaar op een aangewezen locatie aan de wal. De exploitanten van de offshore objecten hebben eigen gespecialiseerde installatie- en onderhoudspartijen. Deze partijen vervoeren de (vervangende) hardware vanaf de aangewezen locatie aan de wal naar de offshore objecten en zorgen voor installatie en onderhoud. De dienstverlening maakt gebruik van bestaande connectiviteit van wal tot platform (bijvoorbeeld glas) van derde partijen. De aanvrager van de dienst zorgt dat deze connectiviteit voor de LAN aansluiting type Offshore beschikbaar is en gebruikt kan worden.

KA LAN (niet meer bestelbaar)

De KA LAN omgeving is bedoeld om ethernet/IP gebaseerde apparaten zoals desktops en servers te koppelen aan RWS VPN's via een Managed LAN. Deze dienst wordt geboden in geconditioneerde ruimtes in RWS kantoorgebouwen en kan alleen worden afgenomen per switch met 24 of 48 KA LAN poorten. Deze dienst wordt vervangen door de LAN aansluiting type KA, waarbij inzet van NAC verplicht is, tenzij er een security exceptie verkregen is. Voor nieuwe bestellingen dient de dienst LAN aansluiting type KA te worden aangevraagd.

KA LAN is opgebouwd uit de volgende componenten:

LAN aansluiting	Lokale LAN poort, gekoppeld in een VLAN, op de Ethernet infrastructuur
Local Area Network	Laag 2 Ethernet VLAN op de Ethernet infrastructuur
Ethernet infra	Ethernet infrastructuur in gebouwen

Op basis van de grootte van de locatie en bijbehorende KA omgeving wordt onderscheid gemaakt tussen 3 type KA LAN waarvan de kenmerken zijn weergegeven in Tabel 10 Opties type KA LAN. Alle locaties zijn geschikt voor één of meerdere VPN aansluitingen.

Opties type KA LAN aansluiting												
Type locatie	Desktop poorten	Server poorten	LAN			MER/SER			Routering	WAN Router		Bladeservers
			10Base-T	100Base-T	1000Base-T	Geen	Één	Meerdere		Enkelvoudig	Dubbelvoudig	
Klein	<=24		✓	✓		✓	✓			✓		
Middelgroot	✓	✓*	✓	✓	✓**		✓	✓		✓	✓	
Groot	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓

Tabel 10 Opties type KA LAN

*Enkele server poorten
**Beperkt aantal 1000Base-T poorten

De KA-LAN omgeving kent de volgende functies:

- Het is mogelijk meerdere VLAN's te creëren op een fysieke poort (trunking). De VLAN's dienen toe te behoren aan één VPN;

- Om de netwerkcapaciteit uit te breiden, is het mogelijk om tussen twee switches port-channeling toe te passen. Hiermee wordt de capaciteit van beide switches gecombineerd;
- Er wordt een spanning-tree protocol toegepast om problemen in het netwerk te detecteren en te voorkomen;
- Het is mogelijk om niet-routeerbare /geïsoleerde VLAN's aan te vragen. Deze VLAN's worden wel administratief gekoppeld aan een VPN Aansluiting;

LAN aansluiting Type KA en LAN aansluiting type Call center

De LAN Aansluiting type KA is bedoeld om ethernet/IP gebaseerde apparaten zoals desktops en servers te koppelen aan RWS VPN's via een Managed LAN. Deze dienst wordt geboden in geconditioneerde ruimtes in RWS kantoorgebouwen. De LAN aansluiting type KA wordt standaard verplicht geleverd mét NAC.
Ten behoeve van Call Center omgevingen is het mogelijk Power over Ethernet (PoE) toe te passen. Hiermee kan een aangesloten apparaat zoals een call center server, bedien PC, telefoon of Wall board via de aansluiting op de switch van stroom worden voorzien.

Wifi

De dienst WIFI biedt veilige draadloze netwerktoegang op RWS locaties die zijn aangesloten op het RWS netwerk. De WiFi dienstverlening ondersteunt de WiFi standaarden WiFi-2 t/m WiFi-6, waarbij overigens alleen WiFi-6 nog nieuw te bestellen is.

Er worden vier gebruikersgroepen onderkend:

- RWS medewerkers met door RWS beheerde mobiele devices voorzien van een RWS certificaat
  kunnen middels de SSID's 'RWS-intern' of 'RijkskantoorRoam' toegang krijgen tot de WiFi dienstverlening van RWS.
  Hiermee kunnen de RWS beheerde mobiele werkplekken draadloos worden verbonden en daarbij logisch dezelfde toegang verkrijgen als via een vaste bedrade kantoor aansluiting (KA).
- Deelnemers van Rijkskantoorroam:
  Deelnemers van Rijkskantoorroam kunnen middels het SSID 'RijkskantoorRoam' toegang krijgen tot de WiFi dienstverlening van RWS die is gekoppeld aan de Rijkskantoor dienstverlening.
- Deelnemers van Govroam, zie https://govroam.nl/ voor actuele deelnemers:
  - Door middel van de overheid brede 'Government roaming Nederland' oplossing wordt gefilterde internettoegang geboden voor alle medewerkers van de overheidsorganisaties die aangesloten zijn op de landelijke Govroam dienstverlening.
  - BYOD RWS medewerkers: Het SSID 'govroam' is voor RWS medewerkers beschikbaar voor BYOD devices.
- Gastgebruikers die akkoord gaan met de algemene voorwaarden van RWS en daarmee zonder identificatie toegang krijgen tot het publieke internet op de door RWS CIV aangewezen locaties

Elke groep kent een specifieke, functioneel andere Service Set Identifier (SSID) zoals weergegeven in Tabel 11 Overzicht gebruikersgroepen WIFI en Open WIFI**.** Het SSID zorgt

voor functiescheiding tussen de verschillende logische draadloze netwerken. SSIDs kunnen worden ingesteld per locatie of specifieke ruimte binnen een locatie. Zo kunnen er op een locatie in verschillende ruimten verschillende SSIDs actief zijn. Het aanvragen van een nieuwe functie binnen een SSID of een geheel nieuw SSID kan uitsluitend via CIV RWS IRN INFRA.

Voor de WiFi dienstverlening zijn een tweetal standaard sets van SSID's opgesteld. Één set is bedoeld voor een RWS-locatie en de tweede set is bedoeld voor een RWS-locatie die is aangemerkt als Rijksverzamelkantoor. Gasttoegang is voor beide locaties een optie.

RWS-locatie:
- SSID 'RWS-intern'
- SSID 'govroam'
- SSID tbv OpenWiFi (per locatie aan te vragen)

RWS-locatie aangemerkt als Rijksverzamelkantoor:
- SSID 'RijkskantoorRoam'
- SSID 'govroam'
- SSID 'RijkskantoorGast'

Omschrijving	Functie	Identiteit bekend	SSID	VPN	Security Zone
RWS beheerd device voorzien van RWS-certificaat	Toegang tot interne RWS applicaties, toegang tot internet via bouwsteen Webproxy.	Ja	RWS-intern	RWS:RWS	Semi-trusted
Stichting Govroam	Toegang internet voor gastgebruikers en RWS medewerkers die gebruik maken van een BYOD	Ja	govroam	RWS:Govroam	Untrusted
Rijkskantoor-roam voor RWS-panden die tevens rijks-kantoorpand zijn	- Voor RWS-medewerkers met een door RWS beheerd mobiel device voorzien van een RWS-certificaat. - Voor IDV-G gebruikers van Rijkskantoorroam.	Ja	Rijkskantoor Roam	- RWS:RWS (RWS-medewerkers) - WAN-i (IDV-G)	Semi-trusted
Gastgebruikers zonder account / Open WiFi	Toegang publiek internet	Nee	Rijkskantoor Gast		Untrusted

Omschrijving	Functie	Identiteit bekend	SSID	VPN	Security Zone
(overige locaties)					

Tabel 11 Overzicht gebruikersgroepen WIFI en Open WIFI

De dienst WIFI voorziet in het ophangen van Access Points (AP's) op locaties waarmee gebruikers een draadloze verbinding kunnen opzetten.

Voor het inrichten van een nieuwe locatie en/of een nieuw gedeelte van een bestaande locatie wordt verplicht een inmeting uitgevoerd (dekking en capaciteit) om te bepalen op welke locaties AP's er geplaatst dienen te worden. De AP's worden op strategische plaatsen gemonteerd en zodanig ingesteld zodat binnen het afgesproken dekkkingsgebied roaming tussen deze AP's mogelijk is. Door de strategische plaatsing van de AP's zal de WiFi-dienstverlening het uitvallen van een enkel AP op kunnen vangen, de naburige AP's zorgen in deze situatie voor herstel van dekking (zie ook uitgangspunten hieronder).
De inmeting is een momentopname, interne verhuizingen kunnen de dekking beïnvloeden. De plaatsing van AP's wordt altijd afgestemd met de gebouwbeheerder.

Uitgangspunten

Voor WIFI gelden de volgende uitgangspunten:

- WIFI is niet bedoeld voor missiekritieke applicaties!
- De WIFI AP's worden middels Power over Ethernet (PoE) voorzien van voeding. PoE wordt door de LAN-aansluiting geleverd.
- WIFI wordt uitsluitend geboden op RWS locaties voorzien van minimaal een vaste VPN aansluiting, aangevuld met een "LAN- of KA-LAN aansluiting";
- Voor het inrichten van WIFI op nieuwe locaties is de afname van een nieuwe VPN aansluiting ten behoeve van het WIFI verkeer vereist;
- De 99,5% beschikbaarheid heeft betrekking op de aanwezige radiodekking op een locatie of in een ruimte. De implementatie van AP's zorgt er voor dat bij uitval van een enkel AP de radiodekking gegarandeerd blijft. Uitval van een enkel AP zal niet tot connectiviteitsverlies leiden, wel zal de beschikbare bandbreedte tijdelijk afnemen.
- De WiFi dienst is geschikt voor Voice, Real-Time en Data toepassingen. Alle toepassingen worden met gelijke prioriteit behandeld;
- Wijzigingen in de omgeving, bijvoorbeeld het plaatsen van wanden of een toename in medewerkers kunnen van invloed zijn op de prestaties van het draadloze netwerk;
- Minimale connectiesnelheid van een client is 12Mbps, lagere snelheden worden niet ondersteund;
- Per AP radio worden maximaal 200 clients ondersteund maar 75 clients wordt als "gezond" gezien;
- RWS is verantwoordelijk voor interne bekabeling en stroomvoorziening.

Randvoorwaarden

De volgende randvoorwaarden zijn van toepassing:

- Voor het leveren van WIFI is een door RWS CIV IRN Infra Netwerken geleverde en door SP-IB beheerde LAN omgeving, op basis van Power over Ethernet (PoE), in het pand vereist, welke is aangesloten op het RWS netwerk via een vaste VPN aansluiting;
- Afhankelijk van de SSID's die nodig zijn op een locatie zal/zullen ook één of meer van de volgende VPN's aanwezig moeten zijn: RWS:RWS bij RWS-Intern, RWS:GOVROAM bij Govroam en/of WAN-i voor Rijkskantoorgast;
- Verkregen gebouwplattegronden die gebruikt worden voor site survey's en voor intekening van dekkingsmetingen dienen door alle betrokken partijen vertrouwelijk te worden behandeld;
- De bekabeling dient te voldoen aan minimaal CAT5E of CAT6 ten behoeve van het aansluiten van Access Points;
- Bij uitbreiding van het aantal Access Points op basis van capacity management dient rekening te worden gehouden met de aanwezigheid van juiste bekabeling (zie boven) en stroomvoorziening. De gebouwenbeheerder is hier verantwoordelijk voor;
- WIFI is afhankelijk van de dienst die de LAN functionaliteit levert. Deze LAN functionaliteit is geen onderdeel van de dienst Wi-Fi. Het aansluiten van een AP vereist een 1Gbps LAN Aansluiting met PoE.

Open WIFI

Open WIFI Is een optionele dienst onder WIFI die open internet toegang biedt zonder identificatie voor alle gebruikers op de gekozen locatie. Open WIFI kan voor twee doeleinden worden ingezet:

- Voor gastgebruikers zonder een tijdelijk account, die akkoord gaan met de algemene voorwaarden die in de vorm van een disclaimer aan hen wordt voorgelegd. Toegang alleen naar publiek internet op de door RWS aangewezen locaties. Hierbij wordt onderscheid gemaakt tussen Westraven LEF en Open WIFI op andere RWS-locaties;

- Open WIFI maakt het ook mogelijk om apparatuur zonder webbrowser (bv. informatiezuilen) met internet te verbinden. Dit vindt plaats o.b.v. het MAC-adres van deze apparatuur. Activatie van een MAC-adres is niet locatie-gebonden. Als Open WIFI voor een locatie wordt opgeheven, dan moeten de MAC-adressen voor deze locatie apart worden verwijderd.

- Open WIFI is alleen mogelijk op locaties met NNV connectiviteit en waar al WIFI dienstverlening aanwezig is. De dienst kan worden aangevraagd voor de hele locatie (default) of een deel ervan (incidenteel). Het is ook mogelijk om de dienst voor een beperkte periode, met een begin- en einddatum, aan te vragen, om bijvoorbeeld een tijdelijke behoefte i.v.m. een event te kunnen invullen. Gerelateerd daaraan is het ook mogelijk om de standaard SSID (WIFI-naam) ''RijkskantoorGast'' locatie specifiek aan te passen zodat de WIFI-naam herkenbaar is voor de gastgebruikers die aan dat event deelnemen.

De totale Open WIFI-dienstverlening is gedimensioneerd (niet gelimiteerd) op max. 1.000 gelijktijdig operationele devices. Bij overschrijding van dit aantal vervallen de beschikbaarheidsgaranties.

Categorie Eindsystemen
De categorie **Eindsystemen** beschrijft verschillende eindsysteemtoepassingen: de Digitale Video aansluiting (Encoder Analoge Camera), AAA Remote Access Groepsprofiel, PPP, TBMS BUS en Draadloze aansluiting.

Beheren Eindsystemen
RWS onderkent de volgende eindsystemen:
1. DVA – Digitale Video Aansluiting
2. Remote Access groepsprofiel
3. PPP Aansluiting
4. Remote Access Gebruiker
5. TBMS Bus
6. AAA
7. Draadloze aansluiting

Quanza IB voert het beheer uit op deze Eindsystemen conform onderstaande SLA.

Eindsystemen Dienstenmatrix								
Type Eindsysteem	Beschikbaarheid				Storingshersteltijd in 95% van de gevallen			
	99.5%	99.7%	99.95%		Service Window Kantoortijden		Service Window 24/7	
	Onbeschikbaarheid per jaar							
	ca 1d20u	ca 1d2u	ca 4u28m		8 uur	4 uur	8 uur	4 uur
DVA – Digitale Video aansluiting		V						V
Remote Access Groepsprofiel			V					V
PPP Aansluiting	NVT				redelijke effort			
Remote Access Gebruiker	NVT				redelijke effort			
TBMS Bus	NVT				redelijke effort			

Tabel 12 Beschikbaarheids eisen Eindsystemen

Bestelbare items en levertijd
Voor de **Eindsysteem toepassingen** gelden de in onderstaande tabel weergegeven bestelbare items met bijbehorende standaard levertijden.

Eindsystemen			
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen (door SP-O&A)**	**SSR (door SP-IB)**
Digitale Video Aansluiting (Encoder Analoge Camera)			
Opheffen incl. installatie	Opheffen dienst op eindsysteem inclusief installatie	10	

Eindsystemen			
Opheffen	Opheffen dienst op eindsysteem exclusief installatie	10	
Wijzigen	Wijzigen instelling Digitale Video aansluiting	5	
PPP aansluiting			
Opheffen	Opheffen PPP aansluiting	10	
Wijzigen	Wijzigen PPP aansluiting	10	
TBMS BUS			
Opheffen	Opheffen TBMS BUS	10	
Remote Access groepsprofiel			
Aanvragen	Aanvragen RAS profiel	20	
Opheffen	Opheffen RAS profiel	5	
Wijzigen	Wijzigen RAS profiel	5	Ja
AAA Ras gebruiker			
Aanvragen	Aanvragen RSA Token	5	
Opheffen	Opheffen RSA Token	5	
Wijzigen	Wijzigen RSA Token	Direct	Ja
AAA NAC Profiel			
Aanvragen	Aanvragen AAA toegang voor devices, applicaties of eindgebruikers	Maatwerk	
Opheffen	Opheffen AAA toegang voor devices, applicaties of eindgebruikers	Maatwerk	
Wijzigen	Wijzigen AAA toegang voor devices, applicaties of eindgebruikers	Maatwerk	
Draadloze aansluiting			
Opheffen	Opheffen Draadloze aansluiting op afstand	5	
Wijzigen	Wijzigen instelling bestaande Draadloze aansluiting op afstand	10	

Tabel 13 Bestelbare items categorie Eindsystemen

Levering gebeurt door Quanza – O&A met uitzondering van de Standaard Service Requests, die door Quanza – IB worden uitgevoerd. Voor alle werkzaamheden op locatie wordt SPIE aangestuurd.

AAA RAS gebruiker, Remote Access groepsprofiel en AAA NAC Profiel

Het doel van de dienst Authenticatie, Autorisatie en Accounting (AAA) is om op gecontroleerde wijze toegang tot het netwerk en/of applicaties van RWS mogelijk te maken.

De dienst AAA doet de controle en verificatie aan de hand van de authenticatie/autorisatie gegevens en bestaat uit de volgende onderdelen:

- **Authenticatie:** de verificatie van de aanmeldgegevens, (de identiteitsgegevens van de eindgebruikers die toegang vragen tot het netwerk of applicaties op het netwerk);
- **Autorisatie:** toekennen van toegangsrechten aan de eindgebruiker;
- **Accounting**: consistente administratie en het kunnen verstrekken van aanmeldinformatie over de eindgebruiker en het gebruik.

De dienst AAA biedt:

- Gecontroleerde toegang voor (netwerk)componenten, applicaties en/of eindgebruikers tot de AAA dienstverlening;
- Gecontroleerde toegang tot het netwerk van RWS voor een gebruiker, of RWS beheer mobiel apparaat voorzien van een RWS-certificaat;
- Gecontroleerde toegang tot het netwerk voor IDV-G (Rijkskantoorroam) waarbij de authenticatie wordt afgehandeld door de IDV-G organisatie. RWs is IDV-P in deze situatie.
- Gecontroleerde toegang tot het netwerk en/of applicaties van RWS voor een gebruiker voor het gebruik van Token of SMS Authenticatie.
- Gebruikersauthenticatie met een RSA token;
- Gebruikersauthenticatie met SMS One Time Password (OTP);
- User account synchronisatie met RWS Active Directory ldap(s);
- Selfservice voor RSA tokens (HTTPS).

AAA RAS gebruiker

Deze dienst biedt de mogelijkheid om iemands identiteit met hoge zekerheid, volgens de 'two-factor authenticatie' methodiek vast te stellen en aan de hand hiervan toegang te geven tot het RWS netwerk.

Hierbij wordt gebruik gemaakt van:

1. Gebruikersnaam (accountnaam);
2. Iets wat een gebruiker 'weet' (kennis);
3. Iets wat een gebruiker 'bezit' (token).

Tokens

Er zijn twee soorten tokens beschikbaar:

1. SMS via de eigen telefoon. De verificatie vindt plaats via het versturen van een S naar het voor die gebruiker in de AD van RWS vastgelegde 06-nummer.
2. Een persoonlijke RSA token voorzien van een unieke code die op het scherm
   van dat token wordt gepresenteerd.

Remote Access Groepsprofiel

Wat een gebruiker of component, na succesvolle authenticatie, mag benaderen op het RWS netwerk wordt bepaald aan de hand van profielen. Deze profielen zijn onderdeel van de dienst Remote Access groepsprofiel. Door het aanvragen van het juiste groepsprofiel is het

mogelijk om via het Internet vanaf een willekeurige locatie en willekeurig apparaat veilig met de binnen het profiel vrijgegeven interne systemen en applicaties van RWS te kunnen werken via een versleutelde verbinding. De dienst is niet bedoeld als machine to machine communicatiemedium.

De dienst Remote Access groepsprofiel is randvoorwaardelijk voor het gebruikmaken van de AAA dienst RAS gebruiker. AAA RAS gebruiker voorziet de gebruiker van een token om succesvol te kunnen authentiseren. In het RAS Profiel zijn de toepassingen en systemen waarvan gebruik gemaakt kan worden gespecificeerd.
Om veiligheidsredenen is de set aan toepassingen en systemen beperkt volgens het 'need to access' principe. In combinatie met de dienst AAA, die een koppeling legt tussen een RAS Profiel, een specifieke Active Directory (AD) user-account en een RAS Token, wordt het mogelijk om succesvol via de RAS dienst op het RWS netwerk in te loggen en de in het RAS profiel beschikbaar gestelde applicaties te gebruiken. Na het succesvol inloggen krijgt de gebruiker een specifieke pagina te zien met daarop de snelkoppelingen (hyperlinks) naar de beschikbaar gestelde interne applicaties en systemen. De inhoud van deze pagina komt overeen met hetgeen in het RAS Profiel was gespecificeerd.
In de RAS server worden RAS profielen conform aanvraag vanuit RWS geconfigureerd. De RAS profielen geven zogezegd toegang tot interne RWS applicaties. De autorisatie van een RAS gebruiker tot een RAS profiel vindt plaats via role mapping.

Voor de dienst RAS Groepsprofiel gelden de in Tabel 14 volgende applicatie en toepassingsvoorwaarden:

Applicatie	Randvoorwaarden gebruiker/randapparaat
Web services (gebaseerd op de http(s) protocollen)	○ Applicaties moeten middels http(s) kunnen werken.
Citrix	○ Citrix ICA Client op Randapparaat
Windows Fileshare/Directories	○ Read-Only (default) of Read-Write. ○ Naar specifieke Share op specifieke Server. ○ Optioneel ook alleen vanaf een specifieke directory (en alle daaronder gelegen directories). ○ Read-Write alleen op basis van een specifieke Risico Analyse. En dit vereist een browser met Java die de Network Connect (*) applicatie kan draaien.
Windows Terminal Services (RDP protocol)	○ Remote Desktop client applicatie (bijvoorbeeld mstsc.exe), ○ user only; hiermee kan men dus niet als admin aanloggen op een remote systeem.
SSH	○ Alleen voor karakter gebaseerde / Virtual Terminal communicatie. ○ Tunneling van andere protocollen is niet toegestaan.

Applicatie	Randvoorwaarden gebruiker/randapparaat
Overige applicaties alleen op basis van transparante netwerktoegang	○ RWS is zeer terughoudend in het toegang verlenen via deze methode, i.v.m. hogere risico's. Deze vorm vereist een specifieke Risico Analyse. ○ Directe communicatie tussen netwerken (Transit verkeer) is expliciet verboden. Hiervoor dient gebruik gemaakt te worden van de dienstbouwsteen Externe Koppeling. ○ Toegang wordt verleend naar specifiek(e) IP adres(sen), Protocol en poort nummer(s). ○ Vereist een browser met Java die de Network Connect applicatie kan draaien.

Tabel 14 Applicatie en toepassingsvoorwaarden RAS Groepsprofiel

De volgende voorschriften gelden voor het definiëren en gebruiken van RAS profielen:

- RAS profielen dienen maximaal van applicatie beveiligingsproxies (bedoeld worden de standaard applicaties zoals rdp, ssh e.d.) gebruik te maken en minimaal van transparante toegang;
- RAS Profielen mogen alleen toegewezen worden aan RAS gebruikers die voor alle applicaties en systemen in het RAS profiel geautoriseerd zijn;
- Het ontsluiten van RWS interne Applicaties en Systemen via de RAS dienst verloopt via een risico afweging en toets ten opzichte van security baseline(s);
- De systeem eigenaar/product manager van de beschikbaar gestelde applicaties, systemen, netwerken en informatie dient expliciet toestemming te geven voor deze netwerk toegang;
- Indien een RAS profiel gebruikt wordt door gebruikers van derde partijen dan moet deze derde partij voldoen aan de NNV aansluitvoorwaarden;
- Ieder RAS profiel dient een benoemde functioneel beheerder te hebben.

Autorisatie middels AAA SMS authenticatie

Voor AAA SMS authenticatie (OTP) wordt voor de profielen de AD benaderd middels LDAPs en is de autorisatie afhankelijk van de AD groepen waar deze gebruiker of dit component deel van uitmaakt. De dienst AAA is beschikbaar voor Verkeersmanagement (VM), het Ministerie van Infrastructuur en Waterstaat (IenW), RWS CIV IRN Infra, BOS en Scheepvaartmanagement (SVM).

De dienst AAA heeft de volgende uitgangspunten:

- De dienst maakt gebruik van een aantal interfaces:
  <u>PIN authenticatie</u>
  - Gebruikers moeten een PIN authenticatie uitvoeren in geval van een RSA-token.

  <u>Token authenticatie</u>
  - De RAS server communiceert met token authenticatie systemen via de RADIUS server;
  - De token authenticatie systemen verifiëren op hun beurt of gebruikers bestaan via een eigen koppeling met de RWS Active Directory;

  - https ingang voor eindgebruikers via een self service portal (SSP) om tokenmanagement uit te voeren (bv pin reset of opgeven van een aflever adres);
  - radius ingang voor de component RAS voor authenticatie en autorisatie van de RAS gebruikers. De autorisatie is een RADIUS attribuut dat de RAS component gebruikt bij mapping op een RAS profiel (met bijbehorende permissies);
  - LDAP(s) uitgang naar de RWS AD omgeving voor het authentiseren van gebruikers die op de SSP inloggen, en voor het synchroniseren van de gebruikersdatabase.
- De dienst ondersteunt de volgende protocollen: TACACS+, RADIUS, LDAPs (Light Weight Directory Access Protocol) en gebruik in combinatie met onder ander PPP , PAP, CHAP, EAP, PEAP, TLS en in bredere zin toegangscontrole middels 802.1x.
- Voor andere componenten en diensten zal per stuk bekeken moeten worden welke interfaces geschikt zijn om van AAA gebruik te kunnen maken. Gebruik van RADIUS of koppeling met de AD middels LDAP(s) behoren tot de mogelijkheden.

Voor de dienstcomponenten van AAA gelden de in Tabel 15 weergegeven voorwaarden:

Dienst component	Voorwaarden
RWS Active Directory	• Gebruiker moet reeds een actief **User-account** hebben in RWS Active Directory. • Bij SMS authenticatie dient het user account ook over een bruikbaar **telefoonnummer** attribuut te beschikken • Bij SMS authenticatie dient het user account ook te zijn opgenomen in een AD groep die correspondeert met een RAS profiel.
Token	• De gebruiker moet een **RSA Token** hebben of krijgen en het serienummer dient daarvan bekend te zijn. Dit is niet van toepassing indien gebruik wordt gemaakt van SMS authenticatie.
Applicaties Autorisatie	• De Gebruiker moet **autorisatie** hebben om de systemen en applicaties te mogen benaderen.
Firewall Rule	• De **Firewalls** dienen de juiste en geautoriseerde toegang mogelijk maken
<ICT-Middelen>	• De Gebruiker moet zelf voorzien in een **internet verbinding**.
	• De Gebruiker moet zelf voorzien in een **ICT-Middel**, zoals een PC, laptop, PDA, smartphone of tablet. De telefoon is essentieel wanneer de gebruiker SMS authenticatie toepast.
	• Het ICT-Middel dient altijd gevrijwaard te zijn van virussen, malware en key loggers; en te voldoen aan het vigerende RWS beveiligingsbeleid.
	• Het ICT-Middel ondersteunt minimaal een standaard **webbrowser** (zoals Internet Explorer of Firefox) met een recente versie (< 3 jaar oud) om de inlogprocedure voor de Remote Access Verbinding te volbrengen.
RAS Gebruiker	• In geval van authenticatie met een 'RSA token', zijn per gebruiker de RWS Active Directory username, het Token-nummer en het RAS Profiel met elkaar gekoppeld. • Wanneer gebruik wordt gemaakt van SMS authenticatie vindt de koppeling plaats via groepslidmaatschap in de RWS active directory en valt de koppeling buiten de dienstbouwsteen

Tabel 15 Voorwaarden dienstcomponenten AAA

Aanvullend geldt het volgende:

- Voor het gebruik van de RSA-Token moet de gebruiker de "Bruikleenovereenkomst ICT-middel" ondertekend hebben. Dit kan middels een notificatie pagina op de Remote Access Service zelf. Dit is niet van toepassing bij het gebruik van SMS tokens;
- RSA tokens en/of telefoons (t.b.v. SMS token codes) mogen niet uit handen gegeven worden;
- RSA tokens dienen niet zichtbaar opgeborgen te worden zodat de gegenereerde tokencodes en het serienummer maximaal afgeschermd zijn voor ongeoorloofde ogen;
- Gebruikers worden geacht geïnformeerd over en bekend te zijn met de fenomenen Social Engineering en Phishing: methoden van afkijken en hoe dit te voorkomen;
- Gebruikers mogen nooit het Token serienummer, PIN-code, tokencode, passcode of wachtwoorden prijsgeven, ook niet aan een helpdesk;
- Gebruikers moeten alert zijn bij het gebruik van sociale media, zodat gevoelige informatie niet indirect prijsgegeven wordt;

- Tokens mogen alleen gebruikt worden op een werkplek met adequate beveiliging tegen malware, keyloggers en screencapture/screenrecorders door middel van anti-malware software;
- Tokens mogen niet gebruikt worden in publieke ruimten zoals cybercafes of op openbare computers;
- Gebruikers moeten bij vermoedens van onrechtmatig gebruik van hun toegang[3], of pogingen daartoe zoals social engineering, dit als security incident melden bij de corporate servicedesk alsmede een directe blokkade aanvragen.

AAA NAC Profiel
Een NAC profiel is een vooraf vastgestelde combinatie van gebruiker, device en gegevens (certificaat/gebruikersnaam-wachtwoord) die bepaalt in welke compartiment (RWS:RWS, WANi, Govroam) dit device of deze gebruiker bij gebruik van de juiste inloggegevens toegang wordt gegeven tot bijbehorende netwerkfaciliteiten (compartiment). Onafhankelijk of deze toegang bedraad of draadloos gevraagd wordt.

Omdat de set gegevens kan wijzigen is het in de PDC mogelijk gemaakt om aanvraag, wijziging en verwijderen van NAC-profielen te bestellen. RWS kan besluiten om gebruik te maken van een nieuw type certificaat, dan betreft het een aanvraag. Ook kan het bijvoorbeeld voor komen dat een realm in een bestaand certificaat type wordt aangepast, dan dient een profiel gewijzigd te kunnen worden. Als RWS besluit om een certificaat type, of authenticatie methode niet meer toe te passen dient deze verwijderd te kunnen worden uit het NAC-profiel.
Het opstellen van een NAC-profiel kan alleen in samenwerking met een Infra adviseur RWS uitgevoerd worden, en bij testen en uitrollen van het NAC-profiel zal RWS middelen ter beschikking dienen te stellen.

Digitale Video aansluiting (niet meer te bestellen)
De Digitale Video aansluiting, weergegeven in Fout! Verwijzingsbron niet gevonden., ten b ehoeve van Analoge Camera’s is bedoeld om analoge Pan Tilt Zoom camera’s aan te sluiten op digitale apparatuur. De PTZ camera’s worden op afstand bestuurd en kunnen worden gedraaid, in- en uitgezoomd en gekanteld. Als onderdeel van deze dienst worden camerabeelden ge-encodeerd en PTZ-signalen gedecodeerd. Het analoge videosignaal type Phase Alternating Line(PAL) wordt standaard omgezet naar een digitaal MPEG2 over IP signaal en het PTZ signaal wordt omgezet naar een serieel RS-485 signaal. Hierdoor kunnen de videobeelden van deze camera’s worden bekeken in de Verkeerscentrales. De dienst is geschikt voor inzet in ongeconditioneerde ruimtes. Daarnaast wordt Multicasting ondersteund waardoor er met meerdere monitoren tegelijkertijd naar één camera gekeken kan worden. Deze dienst gaat altijd vergezeld van een LAN Aansluiting.

De Digitale Video aansluiting kent vier varianten:

[3] Bijvoorbeeld als men een logincode ontvangt via SMS, terwijl men niet aan het telewerken is.

- Variant 1: De Camera is gemonteerd op het portaal en wordt middels koperkabel (COAX) aangesloten op de encoder in de bijbehorende wegkantkast.
- Variant 2: De Camera is gemonteerd op een mast. De encoder is gemonteerd in de camera-aansluitkast en wordt middels multi-mode glasvezelkabel aangesloten op de dichtstbijzijnde wegkantkast.
- Variant 3: De Camera is gemonteerd op een mast. De encoder is gemonteerd in de camera-aansluitkast en wordt middels single-mode glasvezelkabel aangesloten op de dichtstbijzijnde wegkantkast.
- Variant 4: De Camera is gemonteerd op een portaal of mast en wordt middels een enkele single mode glasvezelkabel aangesloten op de dichtstbijzijnde CVR.

Voor het aansluiten van digitale (IP) camera's is een LAN-aansluiting type CVR / VOR of Wegkant/Waterkant bestelbaar. Het demarcatiepunt van deze aansluiting is de LAN-poort. Bekabeling vanaf de LAN-poort naar de camera en eventuele media convertor zijn geen onderdeel van de dienst.

PPP aansluiting (niet meer te bestellen)
Deze dienst biedt een serieel (RS232) koppelvlak voor de weg- of waterkanttoepassingen naar de Backbone bedoeld voor communicatie met de Verkeerscentrale. Deze dienst werd typisch toegepast bij DRIPs, TDIs, VRIs en GMS2 en is geschikt voor ongeconditioneerde ruimtes.

Deze dienst in niet langer te bestellen. Er kunnen nog wel wijzigingen aangevraagd worden en de dienst kan opgezegd worden. De opvolgers van deze dienst zijn de Draadloze VPN Aansluiting en de LAN Aansluiting die beiden uitgaan van een LAN koppelvlak.
De Special "PPP met huurlijnverlenging" kan niet worden aangevraagd noch gewijzigd, deze kan alleen worden opgezegd.

TBMS BUS (niet meer te bestellen)
TBMS staat voor Token Bus Master Slave en is een op 802.4 (Token passing) gebaseerd protocol met een door RWS gemodificeerde TCP/IP stack (VOPP) bedoelt voor de specifieke eisen van de wegkantsystemen ((M)WKS).
Deze netwerktoegangsdienst maakt het mogelijk dat wegkantstations, die gebruik maken van partylines, voor de applicatie 'Monica' via het TBMS protocol gekoppeld kunnen worden aan het generieke op ethernet/IP gebaseerde RWS netwerk.

Deze dienst in niet langer te bestellen en er kunnen geen wijzigingen meer aangevraagd worden. De dienst kan uitsluitend opgezegd worden. De SLA van de TBMS dienstverlening is op basis van 'redelijke inspanning'. Onbeschikbaarheid van spare apparatuur kan ertoe leiden dat een storing niet meer kan worden opgelost en een verstoorde TBMS-dienst daarom niet meer operationeel gekregen kan worden.

Draadloze aansluiting (niet meer te bestellen)
De Draadloze aansluiting betreft een aansluiting gebaseerd op een serieel koppelvlak en TCP/IP PPP (point to point protocol) en werd toegepast voor het aansluiten van weg- of waterkant toepassingen als DRIPs, TDI's en Meetnetaansluitingen met een serieel koppelvlak. Omdat er gestreefd wordt naar een all-IP netwerk, wordt dit koppelvlak als 'legacy' gecategoriseerd en is niet meer bestelbaar. De Draadloze aansluiting bestaat uit een (ruggedized) draadloos modem + SIM (Wireless 2G/RS232).

Voor inbouw in weg- of waterkanttoepassingen gelden veelal specifieke montagevoorschriften. Zie hiervoor de desbetreffende documentatie (beschikbaar op de VPR).

Categorie Overig
De categorie Overig biedt een overzicht van de informatie diensten glas en netwerk, ontwerp diensten, impact analyses en RijkskantoorRoam: Rijksverzamelkantoor netwerk functionaliteit op een RWS Kantoor (Provider) en RWS netwerk functionaliteit op een niet RWS (Rijks)Overheid Kantoor (Gebruiker) gebaseerd op standaard PDC Diensten.

Gepland werk Glas
Indien bij aanleg- of renovatieprojecten mutaties in het glasvezelnetwerk van RWS noodzakelijk zijn, dienen aannemers deze activiteiten uit te voeren op basis van een glasadvies van SP-O&A.

Er wordt onderscheid gemaakt tussen de volgende gradaties gepland werk (Tabel 16):

Gepland Werk Glas		
Type	**Kenmerken**	**Deliverables**
Eenvoudig (zonder additionele kosten aan te vragen als RFI)	Als elk punt van toepassing is: * < 4 uur analyse * < 4 uur begeleiding * Begeleiding tijdens kantooruren * * Max. één overleg met RWS-Opdrachtnemer Verwachte tijdsbesteding max 16 uur	* Overzicht van de bezette vezels in de betrokken kabels * Opsomming welke PDC-diensten 'geraakt' worden * Enkelvoudig gerouteerd, zoals camera's * Dubbel gerouteerd, zoals aansluiting via ELDW * Aansluitingen van derden in beheer bij OPSI * Aansluitingen van derden niet in beheer bij OPSI * Onbekende aansluitingen (bezet zonder bekende PDC-dienst of naam gebruiker) * Analyse of de geraakte dubbel-gerouteerde PDC-diensten niet 'toevallig' ook betrokken zijn bij andere werkzaamheden of lopende incidenten. * Analyse welke andere SI's dan DVM-Droog worden geraakt waardoor ook derden geïnformeerd moeten worden en mogelijk CAB ingeschakeld moet worden. * Review Plan van Aanpak RWS-ON * Begeleiden her-indienststelling switches * Informeren SI's en afstemmen met CAB
Standaard	Als één punt van toepassing is: * > 4 uur analyse * > 4 uur begeleiding * Begeleiding buiten kantooruren * * Meer dan één overleg met RWS-Opdrachtnemer Verwachte tijdsbesteding max 40 uur	

Gepland Werk Glas		
Type	**Kenmerken**	**Deliverables**
Projectmatig Small	Als van toepassing is: *Projectmatige begeleiding gewenst en *Vooronderzoek ter plaatse of vooraf testen en/of fysiek vrij schakelen van verbindingen of lokale begeleiding tijdens de werkzaamheden. *Eén dagdeel een monteursteam van 2 man. *Werkzaamheden gedurende max één dag op één tracé. Verwachte tijdsbesteding totaal max 80 uur.	* De onder 'eenvoudig' en 'standaard' genoemde deliverables, en tevens: * Projectcoördinator voor voorbereiding en begeleiding van de werkzaamheden; * Verificatie vooraf in technische ruimtes (CVR e.d.) of bezetting van de kabels overeenkomst met administratie. Control met 'lichttang' of vezels daadwerkelijk bezet zijn. * Verificatie vooraf in technische ruimtes (CVR e.d.) of het vrij schakelen van een verbinding het verwachte effect heeft (testen). * Test op redundantie van verbindingen vooraf (op locatie en/of via beheerssysteem) * Vooraf omsteken van verbindingen in technische ruimtes (CVR e.d.) indien dit uit oogpunt van handhaven verbinding gewenst is. * Vrij schakelen en terugschakelen van verbindingen op de dag van uitvoering. * Tijdens de uitvoering zijn monteurs en een projectcoördinator op locatie aanwezig. * Tijdens de uitvoering zijn een netwerkbeheerder en een back-up beschikbaar voor test en controle via de netwerkmanagementsystemen. Niet inbegrepen is het opgraven, openen en onderzoeken van kabelputten. Dit kan als meerwerk uitgevoerd worden.
Projectmatig Medium	Als van toepassing is: *Projectmatige begeleiding gewenst en *Vooronderzoek ter plaatse of vooraf testen en/of fysiek vrij schakelen van verbindingen of lokale begeleiding tijdens de werkzaamheden. *Drie dagdelen een monteursteam van 2 man. *Werkzaamheden gedurende max één dag op één tracé. Verwachte tijdsbesteding totaal max 130 uur.	
Projectmatig Large	Als één punt van toepassing is: * Meer dan drie dagdelen inzet van een monteursteam. *Werkzaamheden gedurende meerdere dagen *Werkzaamheden op meerdere tracés. Verwachte tijdsbesteding totaal > 130 uur.	

Tabel 16 Gepland werk Glas

Glasadvies

Het glasadvies is bedoeld om in een project, voorafgaand aan de bestelling van PDC-diensten, de aanvrager te ondersteunen in het maken van de juiste keuzes. Uitgangspunt is dat er uitgegaan kan worden van bestaande netwerkarchitectuur, technologie en apparatuur.
Daarnaast wordt beoogd:

- Adequate voorbereiding te doen voor de datanetwerken in een RWS-project om latere bestelling en levering van PDC-diensten snel, effectief en efficiënt mogelijk te maken;
- De opdrachtnemer van RWS te ondersteunen in het maken van de juiste keuzes bij het aanleggen van glasvezelinfrastructuur of benutten van bestaande glasvezelinfrastructuur voor datanetwerken, waarmee een goed te beheren en toekomst vast datanetwerk ontstaat.

Er wordt onderscheid gemaakt tussen drie type adviezen:

Glasadvies		
Type	Kenmerken	Deliverables
Eenvoudig	* <= 2 overleggen *<= 4 lassenleiding tijdens kantooruren * *<= 20km netwerk * Bestaande technologie * Bestaande beheeromgeving	* Advies routering nieuwe infra * Advies gebruik bestaande infra * Advies posities glasvezelkabelputten en kasten * Lasschetsen en routeringsschema uit Cocon * Aanwijzing gebruik glasvezellades in CVR e.d. * Advies te bestellen typen PDC-items * Advies en bestemming over eventuele fasering uitvoering * Afstemming met andere lopende projecten * Adviesrapport
Complex	* <= 4 overleggen *<= 10 lassenleiding tijdens kantooruren * *<= 50km netwerk * Bestaande technologie * Bestaande beheeromgeving	

Maatwerk	* Meer afstemming
	* Groter netwerk
	* Afwijkende technologie
	* Nieuwe beheeromgeving
		Als hierboven, aangevuld met:
		* Inventariseren afwijkende bedrijfsmiddelen
		* Advies posities glasvezelkabelputten en kasten
		* Advies hoe om te gaan met niet-acceptabele afwijkingen
		* Afstemmen en inregelen:
		  * Incidentbehandeling
		  * Onderhoud
		  * Changemanagement
		* Inventariseren gebruik glas door niet-PDC-diensten
		* Eventueel opstellen maatwerk-DAP

Tabel 17 Glasadviezen

Netwerkadviezen
Indien blijkt dat de functionele behoefte niet ingevuld kan worden met PDC leveringen dan dient het Service Portfolio Management proces gestart te worden om te komen tot een nieuwe of gewijzigde dienst.

Uurtarieven
Als onderdeel van de dienstverlening biedt SP-O&A de inzet van medewerkers aan bij Projecten en Leveringen. De uurtarieven van onderstaande rollen zijn beschikbaar in het Prijzenblad. In het geval van Leveringen wordt gebruik gemaakt van een strippenkaartconstructie. In een 'Strippenkaart' wordt een aantal uren per rol aangeboden, welke op basis van werkelijk gemaakte uren worden verrekend. De afnemer wordt tijdig op de hoogte gebracht bij dreigende overschrijding van de geplande uren.

Rol	Specificatie
Senior Engineer	Senior netwerk engineer

Rol	Specificatie
Engineer	Medior netwerk engineer verantwoordelijk voor het uitvoeren van wijzigingen
Projectleider	De projectleider coördineert PDC- aanvragen en projecten
Project Coördinator	Project Coördinatoren worden ingezet in dienstontwikkelingstrajecten, zowel in de pre-sales als in de projectfase voor het coördineren van dienstontwikkelingsprojecten.
Project Support	Ondersteuning van projecten, zoals PMO-rollen

Tabel 18 Uurtarieven

Bestelbare items en levertijd Informatie- en ontwerpdiensten

Informatie en ontwerp diensten		
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen (door SP-O&A)**
RFI Glas	Informatieverzoek m.b.t. het RWS glasvezelnetwerk	5
Impactanalyse Glas	Beschrijft de impact van een wijziging aan de RWS glasvezel-infrastructuur	20
Glasadvies	Technisch advies over een wijziging aan de RWS glasvezel-infrastructuur	20
Glasontwerp	Technisch detailontwerp voor een wijziging aan de RWS glasvezelinfrastructuur	20
RFI Netwerk	Informatieverzoek m.b.t. de RWS IT-netwerkinfrastructuur	5
Impactanalyse Netwerk	Beschrijft de impact van een wijziging aan de RWS IT-netwerkinfrastructuur	20
Netwerkadvies	Technisch advies over een wijziging aan de RWS IT-netwerkinfrastructuur	20
Netwerkontwerp	Technisch detailontwerp voor een wijziging aan de RWS IT-netwerkinfrastructuur	20

Tabel 19 Bestelbare items Informatie en Adviesdiensten

Levering gebeurt door Quanza – O&A met uitzondering van de Standaard Service Requests, die door Quanza – IB worden uitgevoerd. Voor alle werkzaamheden op locatie wordt SPIE aangestuurd.

Rijkskantoorroam
De dienst Rijkskantoorroam maakt het mogelijk om RWS panden die zijn aangewezen als Rijksverzamelkantoor te voorzien van een Generieke netwerk infrastructuur Connectivity (RijkskantoorRoam). Anderzijds wordt met deze dienst ook de mogelijkheid geboden om RWS medewerkers gebruik te laten maken van de Generieke netwerk infrastructuur Connectivity in Rijksverzamelkantoren van andere Rijksoverheidsorganisaties.
Rijkskantoorroam is een zogenaamde geïntegreerde dienst; hij wordt samengesteld uit de reeds bestaande diensten VPN aansluiting, WIFI, KA LAN, Virtual Firewall, AAA.

Bestelbare items en levertijd RijkskantoorRoam

RijkskantoorRoam		
Eenmalige dienst	**Toelichting**	**Levertijd in werkdagen**
Aanvraag RijkskantoorRoam Provider	standaard Netwerk type Kantoor (redundant en inclusief Wifi) aangevuld met eventuele extra diensten VPN, Virtual Firewall, VPN aansluiting, NAC Profiel, LAN aansluiting type KA en WIFI	In overleg
Opheffen RijkskantoorRoam Provider	Opheffen geïntegreerde diensten	In overleg
Aanvraag RijkskantoorRoam Gebruiker	Een ander (Rijks)Overheid Netwerk aangevuld met de diensten Virtual Firewall en NAC Profiel	In overleg
Opheffen RijkskantoorRoam Gebruiker	Opheffen geïntegreerde diensten	In overleg

Tabel 20 Bestelbare items Rijkskantoorroam

Levering gebeurt door Quanza – O&A. Voor alle werkzaamheden op locatie wordt SPIE aangestuurd.

Beheren IT-netwerkdiensten (Specials)

De Specials bestaan uit:

Verbindingen Lichteiland Goeree – Europlatform

SP-IB levert connectiviteit op de RWS platformen voor de kust van Rotterdam. Ten behoeve van het transport van meetgegevens op de Noordzee wordt gebruik gemaakt van een straalverbinding tussen twee lichteilanden: Lichteiland Goeree (LEG) en Europlatform (EPL).

Service level element	Service level
Beschikbaarheid	
Doelbeschikbaarheid	99,5%
Servicewindow	E8 (365*7*24)
Openstellingtijden servicedesk	24*7 per e-mail en telefonisch
Storingshersteltijd gerekend vanaf vertrek helikopter	95% binnen 16 uur bij dienst verstoord 95% binnen 8 uur bij dienst onderbroken
Maintenance Window	10:00-15:00 in overleg met MKO
Capaciteit	
Throughput	LEG: 10Mb/s EPL: 2Mb/s
Prestaties	
MTU	1.500 Bytes
Packet loss	< 2%
Delay (RTT) typical	< 2ms
Jitter	Delay+jitter < max delay
Convergentiesnelheid	<60s
Multicast support	Ja

Tabel 21 LEG EPL Special

CCM aansluiting

De CCM aansluiting is een VPN Aansluiting Serieel op de CCM server. Het betreft een server die in VicNet staat ten behoeve van camerabediening PTZ. Deze Special kan niet worden aangevraagd of gewijzigd.

Eenmalige Dienst	Toelichting	Levertijd in werkdagen
Opheffen	Beheer Verbindingen LEG-EPL	In overleg
Opheffen	CCM Aansluiting	In overleg

Tabel 22 Bestelbare items Specials

Totaal overzicht SLA Matrix

SLA MATRIX STORINGSHERSTELTIJDEN									
Diensten	Storingshersteltijd in 95% van de gevallen								
	verstoord					onderbroken			
	service window kantoortijden			service window "24/7"		service window kantoortijden		service window "24/7"	
	16	8	4	8	4	8	4	8	4
IDS/IPS				V					V
DWDM				V					V
Mailrelay				V					V
Forward webproxy				V					V
VPN		V		V		V			V
Virtual firewall				V					V
DDI - DHCP & DNS				V					V
DDI - IPAM				V					V
DMZ en DMZ client				V					V
VPN aansluiting				V			V		V
Draadloze VPN aansluiting				V					V
Externe koppeling	V					V			
RKN aansluiting		V							V
Lan aansluiting type Gebouw	V			V			V		V
Lan aansluiting type KA	V			V			V		V
Lan aansluiting type Rekencnt	V			V					V
Lan aansluiting type SPAN	V			V			V		V
Lan aansluiting type CVR/VOR				V					V
Lan aansluiting type Callcenter				V					V
Lan aansluiting type Wegkant/Waterkant				V					V
Lan aansluiting type Offshore	-	-	-	-	-	-	-	-	-
Lan aansluiting type ODC				V					V
KA LAN				V			V		V
WIFI		V				V			
Open WIFI		V				V			
Digitale Video Aansluiting				V					V
Remote Access groepsprofiel				V					V
AAA RAS Gebruiker		V					V		
AAA NAC Profiel				V					V
PPP aansluiting*	-	-	-	-	-	-	-	-	-
TBMS BUS*	-	-	-	-	-	-	-	-	-
Draadloze aansluiting*	-	-	-	-	-	-	-	-	-
LEG EPL				V					V
CCM aansluiting				V					V

*	Op basis van 'redelijke inspanning'

Tabel 23 Storingshersteltijden van de verschillende netwerkdiensten

Bijlage A Afkortingen en Begrippen

Afkortingen

Overzicht van de in deze catalogus gebruikte afkortingen en hun betekenis.

Afkortingen	
RWS	Rijkswaterstaat
RWS CIV IRN Infra Netwerken	Rijkswaterstaat Centrale Informatie Voorziening Infrastructuur Netwerken
NNV	Nieuwe Netwerk Voorzieningen
VPN	Virtual Private Network
DDI	De dienst die bestaat uit DHCP DNS en IPAM
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Services
IPAM	Internet Protocol Adres Management
DMZ en DMZ Client	een Demilitarised Zone (beveiliging laag) en Demilitarised Zone Client (DMZ Aansluiting)
NTP	Network Time Protocol
WoL	Wake on LAN
IPsec	Internet Protocol Security
VO LAN	VPN Ontsluiting LAN
CE	Client Edge
LAN	Local Area Network
KA-LAN	Kantoor Automatisering LAN
CVR	Centrale VicNet Ruimte
VOR	VicNet Object Ruimte
ODC	Overheid Data Center
VC/VP	Verkeerscentrale/Verkeerspost
VLAN	Virtueel LAN (VLAN)
DRIP	Dynamisch Route Informatie Paneel
DOV	Dynamische Openbare Verlichting
TDI	Toerit Dosering Installatie
VRI	VerkeersRegel Installatie
VAD	Vluchthaven Aanwezigheid Detectie
WIM	Weigh in Motion (ten behoeve van het wegen van vrachtwagens)
CADO	Calamiteiten Doorsteek
MTV	Motorway Traffic Video
UWP	Universeel Wegkant Platform
LEF	Het Future Center van RWS waar innovatie centraal staat. LEF is geen afkorting, maar staat voor lef, durf en moed. Voor het verleggen van grenzen
SSID	Service Set Identifier
AP's	Access Points
QoS	Quality of Service
APN	Access Point Name
Wi-Fi	Wireless Fidelity

Afkortingen	
AAA	Authenticatie Autorisatie Accounting
WLAN	Wireless Local Area Network
LCM	Lifecycle Management
FEP	Front End Processor
PTZ	Pan Tilt Zoom
PAL	Phase Alternating Line
IP	Internet Protocol
SIM	Subscriber Identity Module
MTM	Motorway Traffic Management
PLCS	Party Line Crossover Switch
ON	Opdracht Nemer
RSA	Merknaam
RAS	Remote Access Services
OTP	One Time Password
AD	Active Directory
RDP	Remote Desktop Protocol
LDAP	Lightweight Directory Access Protocol
VWS	Verkeersmanagement Services
IenW	Infrastructuur en Waterstaat
SVM	Scheepvaart Management
SSP	Self Service Portal
GMS	Gladheidsmeldsystemen
TBMS	Token Bus Master Slave
WKS	Wegkant Systemen
MWKS	Mobiele Wegkant Systemen

Tabel 24 Afkortingen

Begrippen

Toelichting op de in deze catalogus gebruikte begrippen.

Begrippen	
Prijzenblad	Overzicht van alle bestelbare items inclusief eenmalige kosten en abonnementen
Categorie VPN	Alle diensten welke onderdeel uitmaken van de categorie Virtual Private Network
Categorie VPN Aansluiting	Alle diensten welke onderdeel uitmaken van de categorie Virtual Private Network Aansluiting
Categorie LAN Aansluiting	Alle diensten welke onderdeel uitmaken van de categorie Local Area Network
Categorie Eindsysteem	Alle diensten welke onderdeel uitmaken van de categorie Eindsysteem (toepassingen voor eindsystemen)
Categorie Backbone	Alle diensten welke onderdeel uitmaken van de categorie Backbone/Core/CV omdat deze onderdeel uitmaken van het backbone netwerk van Rijkswaterstaat en uitsluitend door RWS CIV te bestellen zijn
Categorie Special	Alle diensten welke geen onderdeel uitmaken van de Categorie VPN, VPN Aansluiting, LAN Aansluiting, Eindsysteem en Backbone en uitsluitend door RWS CIV te bestellen zijn

Begrippen	
RWS netwerk	Het netwerk van Rijkswaterstaat voorheen bekend als "Rijkswaterstaat Nieuwe Netwerk Voorzieningen"
Object Access Netwerken	Object LAN
Kunstwerken	Rijkswaterstaat benaming voor objecten als bruggen, sluizen, tunnels
Huurlijnen	Transmissielijnen van andere partijen dan Rijkswaterstaat zelf, waarover verkeer van Rijkswaterstaat loopt
Aansluitvoorwaarden NNV (CIV)	De voorwaarden waaraan moet worden voldaan om gebruik te maken van het RWS netwerk
Bulklevering	Levering van een groot aantal bestelbare items in één bestelling
Service Portfolio Management proces	Het proces ingericht om het dienstenportfolio up to date te houden, nieuwe diensten te ontwikkelen, bestaande diensten aan te passen en verouderde diensten uit te faseren
Internet Access	De VPN functie die het mogelijk maakt om toegang tot het internet te verkrijgen
DDI	De dienst die bestaat uit DHCP DNS en IPAM
Mail relay	Configuratie die het mogelijk maakt e-mail berichten te versturen via een SMTP-server
Virtual Firewall	Firewall service in een virtuele omgeving die doormiddel van software communicatie controleert
NTP	Network Time Protocol: maakt het mogelijk om de interne klok van computers met elkaar te kunnen synchroniseren
RWS Backbone	Centrale netwerk-infrastructuur van Rijkswaterstaat
Ruggedized	Verharde apparatuur geschikt voor ongeconditioneerde ruimten
Shaping	Methode om bandbreedte te verdelen zodat data niet verloren gaat en er geen capaciteitstekort ontstaat
Transmissie	Doorlaten van verkeer via verbinding
Wake on LAN	Netwerkstandaard waarmee het mogelijk is een computer op afstand te benaderen
Encrypted Tunnel	Een beveiligde Internet verbinding waarover data versleuteld verzonden wordt
IPsec	Internet Protocol Security
IPsec Gateway	Internet Protocol Security netwerkpunt dat voorziet in toegang tot een netwerk
Externe locatie	Locatie buiten het RWS netwerk
CE domein	Een Custom Edge Router domein
VO LAN	VPN Ontsluiting LAN Configuratie op de router om de LAN-aansluiting te ontsluiten naar het VPN
VPR	RWS SharePoint
LAN domein	Gescheiden deel van het Local Area Network
Routering	Het bepalen van de route die door informatie via het netwerk wordt afgelegd
Centrale VicNet Ruimte	voornamelijk kleine gebouwen op knooppunten van snelwegen waarbinnen een geconditioneerde ruimte aanwezig is voor actieve netwerk apparatuur. Dit betreft een oude benaming die voorlopig vanwege de herkenbaarheid wordt gehandhaafd.

Begrippen	
VicNet Object Ruimte	dit zijn geconditioneerde ruimtes voor actieve netwerk apparatuur binnen objecten zoals tunnels, sluizen, bruggen, radarposten en dergelijke. Dit betreft een oude benaming die voorlopig vanwege de herkenbaarheid wordt gehandhaafd.
LAN ontsluiting	de logische koppeling naar een specifiek VPN
VLAN	Virtueel LAN in de fysieke infrastructuur (bijvoorbeeld de switches)
LAN Aansluiting	de fysieke poort die toegang biedt naar het virtuele LAN
Ethernet infra	dit is de fysieke infrastructuur (bekabeling en switches)
RWS Netwerk LAN	Alle LAN Aansluitingen in het Rijkswaterstaat netwerk met uitzondering van KA-LAN, ODC LAN en WIFI
Duplex instelling	Het protocol voor verzenden en ontvangen van informatie op de LAN Aansluiting
Trunking	Meerdere VLAN's op één fysieke poort
Port channeling	Combineren van de capaciteit switches
Spanning-tree protocol	Protocol dat er voor zorgt dat er slechts één pad mogelijk is voor het zenden van informatie, waarmee ontvangst gegarandeerd wordt.
loop-free topologie	Netwerk waarin loopvorming niet mogelijk is
PTZ Camera	op afstand bestuurbare camera die kan worden gedraaid, in- en uitgezoomd en gekanteld

Tabel 25 Begrippen

Bijlage B Overzicht tabellen

Tabel 1 IT-netwerkdiensten CIV Klant 7
Tabel 2 VPN functionaliteiten 10
Tabel 3 Dienstenmatrix VPN – diensten 10
Tabel 4 Bestelbare items VPN diensten 12
Tabel 5 Dienstenmatrix categorie VPN - aansluiting 13
Tabel 6 Bestelbare items categorie VPN aansluiting 15
Tabel 7 Vaste verbindingen ODIDO 27
Tabel 8 Beschikbaarheids eisen LAN aansluiting 29
Tabel 9 Bestelbare items categorie LAN aansluiting 30
Tabel 10 Opties type KA LAN 33
Tabel 11 Overzicht gebruikersgroepen WIFI en Open WIFI 36
Tabel 12 Beschikbaarheids eisen Eindsystemen 38
Tabel 13 Bestelbare items categorie Eindsystemen 39
Tabel 14 Applicatie en toepassingsvoorwaarden RAS Groepsprofiel 42
Tabel 15 Voorwaarden dienstcomponenten AAA 44
Tabel 16 Gepland werk Glas 48
Tabel 17 Glasadviezen 49
Tabel 18 Uurtarieven 50
Tabel 19 Bestelbare items Informatie en Adviesdiensten 51
Tabel 20 Bestelbare items Rijkskantoorroam 51
Tabel 21 LEG EPL Special 52
Tabel 22 Bestelbare items Specials 52
Tabel 28 Storingshersteltijden van de verschillende netwerkdiensten 53
Tabel 29 Afkortingen 55
Tabel 30 Begrippen 57

Bijlage C Overzicht figuren

Figuur 1 Scope IT-netwerkdiensten 4
Figuur 2 Schematische weergave van de VPN aansluiting 15
Figuur 3 Beschikbaarheid VPN Aansluiting 17
Figuur 4 Standaard routering VPN Aansluiting 18
Figuur 5 Statische routering VPN Aansluiting 18
Figuur 6 Dynamische routering - VPN Aansluiting Connect 19
Figuur 7 Dynamische routering - VPN Aansluiting InterConnect 20
Figuur 8 Schematische weergave draadloze VPN Aansluiting 22
Figuur 9 IPSEC 24
Figuur 10 IPsec + MCPE 25
Figuur 11 Voorbeeld redundante vaste verbinding 25