Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Marktconsultatie connectiviteitsdiensten Justitienet 4
nummer 01 , d.d. 2018-04-03

CBO-Rijk Dataverbindingen

Bezoekadres
Rijkswaterstaat CIV
Derde werelddreef 1
2622 HA Delft

Postbus 556
3000 AN Rotterdam

Meer informatie
ON2013@rws.nl

Kenmerk	Marktconsultatie Connectiviteitsdiensten Jusitienet 4
Perceel	

1	**Gegevens aanbesteding**
Naam aanbesteding	Connectiviteitsdiensten Justitienet 4

2 Informatie

Nr	Vraag	Antwoord
B.	**Visie en Ontwikkeling**	
	Achtergrond B.1. t/m B.11.: Met de uitkomsten van het onderdeel Visie en Ontwikkeling wil RWS CIV vaststellen of de strategie omtrent de verwerving van de dienstverlening vormgegeven kan worden. Voorspellen van de toekomst is lastig, toch de vraag aan de leverancier hoe deze denkt dat de netwerken er over rond het jaar 2025 uit kunnen zien.	
B.1	Ziet de leverancier verschillende toekomstscenario's, en welke scenario's zijn het meest waarschijnlijk?	• Het koppelen van publieke Cloud providers • Benutten van voordelen van nieuwe typen netwerken zoals: Software Defined Netwerken, Netwerk virtualisatie, Flexible Ethernet • 5G zal zijn intrede doen: dat leidt tot hogere mobiele bandbreedtes, die allerlei nieuwe toepassingen en gebruiksvormen ontsluiten • Hybride netwerken waarbij er een duaal netwerktopologie wordt opgezet tussen bijvoorbeeld Private IP (MPLS) en (publiek) Internet gebaseerde netwerken • Volledig (publiek) internet gebaseerde netwerken • Smart City en IoT toepassingen • Security geïntegreerd in het netwerk • Vaste telefoniediensten (VoIP en unified communications) zullen getransporteerd worden over één van hierboven genoemde netwerken, dit met een voorkeur van MPLS omwille van de end-to-end garantie en performance van tijd kritische applicaties. • Overal altijd online op ieder device • In toenemende mate zal self-service door de zakelijke eindgebruiker gaan toenemen. Met als gevolg flexibel inzetten van capaciteit en verhoogde beschikbaarheid • Uitbreiding van de Quarantaine faciliteiten om flexibel en fijnmazig in te kunnen spelen op calamiteiten • Private IP VPN, gebaseerd op het MPLS protocol • Het gebruik van IP VPN's voor verschillende doeleinden, onder andere als beveiligingscompartiment • Het bieden van beveiligde connectiviteit van de crypto in het end-point (e.g. terminal van de gebruiker). • Vereenvoudiging van de administratieve processen (inkoop, facturatie en factuur controle).
B.2	Wat zijn de factoren die deze scenario's bepalen?	• De applicaties die over het netwerk getransporteerd worden en de eisen om hier de nodige garanties, end-to-end, te kunnen leveren (t.a.v. latency, jitter en packet loss) • Hogere bandbreedte eisen • Trend m.b.t. 'shift naar de cloud' (public/hybrid/private) • Flexibiliteit en schaalbaarheid om snel te kunnen inspelen op de behoefte van klanten • Prijsontwikkelingen en budget (meer bandbreedte voor minder of hetzelfde budget) • Verandering van de markt (fusies en overnames) als gevolg van combineren en doorontwikkeling van nieuwe diensten • Centrale en steeds voornamer wordende rol van beveiliging. Bouw hiervoor ruimte in om deze door te doorontwikkelen in de looptijd van het contract. • Cybersecurity: we zien dat er steeds meer geavanceerdere dreigingen en digitale aanvallen plaatsvinden op Nederlandse overheidsnetwerken en websites. • Nationale en internationale wet- en regelgeving: een mooi voorbeeld is de Algemene Verordening Gegevensbescherming (AVG) • Rol en belang nationale veiligheid: zodra de (nationale) veiligheid in het geding komt, zijn overheden minder geneigd om nieuwe ontwikkelingen te stimuleren. • Adoptie van nieuwe technologie • Veranderende (informatie)behoefte eindgebruiker • Flexibiliteit in de trend of ontwikkeling • Beschikbaarheid van gekwalificeerd personeel: nieuwe ontwikkelingen worden afgeremd indien ze te complex en/of moeilijk te beheren zijn. • Legacy van oude netwerken • Kosten: nieuwe technologische ontwikkelingen moeten ook met innovatieve business cases kunnen worden ondersteund • Integratie mogelijkheden: nieuwe ontwikkelingen moeten aansluiten op bestaande omgevingen om succesvol te kunnen worden geïmplementeerd • Snelheid: de snelheid van technologische ontwikkelingen • Marktontwikkelingen en marktbehoeften; • Technologische ontwikkelingen; • Innovatiekracht van partijen;

2 Informatie

Nr	Vraag	Antwoord
B.3	Wat zijn factoren met grote impact, Welke factoren zijn het meest onzeker?	<u>Grootste Impact:</u> • Nationale veiligheid • Cybersecurity • Integratie mogelijkheden • Kosten • Technologische ontwikkelingen • Security policy • Er zullen veel systemen een koppeling maken met het publieke Internet (IoT). Daarnaast zullen veel systemen gemigreerd worden naar een on-premise omgeving binnen de virtuele/cloud omgeving. Security zal hierin één van de grote uitdaging worden. • Los van de ontwikkeling van de techniek willen eindgebruikers gebruik willen maken van gecombineerde verrijkte en Over-The-Top (OTT) diensten. • Bepalend is hoe de zogenaamde big seven (bedrijven zoals Google, Amazon en Microsoft) hierin een bepalende rol gaan spelen, aangezien ze al een groot netwerk hebben en deze kunnen (zullen) gaan gebruiken om meer bedrijven over te halen om workloads te plaatsen op hun cloud platform. <u>Meest onzekere factoren:</u> • Wetgeving • Cybersecurity • Nieuwe businessmodellen • Marktbehoeften • Time to market • Beleid van de overheid m.b.t. faciliteren digitale economie en haar rol daarbinnen
B.4	Welke toekomstige innovaties en/of uitfaseringen ziet u?	<u>Innovaties:</u> • De verwachting is dat nieuwe typen netwerken zoals Software-defined WAN (SD WAN), Netwerk virtualisatie, Flexible Ethernet en On-Demand netwerkdiensten toekomstige innovaties zullen bepalen. • Cloudification en SDN: Een gefaseerde transitie van fysieke netwerken naar gehoste en extern gemanagede omgevingen zal de traditionele rolverdeling tussen gebruiker en leverancier significant veranderen. • On Demand services, het opschalen danwel downgraden van de bandbreedte naar behoefte; bijvoorbeeld op een specifieke tijdstip (of tijdsduur) van de dag. • Automation Operation Support System (OSS)/ Business Support System (BSS): Het managen van het netwerk wordt in mindere mate gedaan door de providers en meer door de klant. Door automatisering krijgt de klant meer grip op product management, customer management en order management. • Telemetry-based assurance: Alle events in het netwerk worden opgeslagen en geanalyseerd • Gigabit snelheden door DOCSIS 3.1 over COAX • 5G als drager voor IPVPN. Met de komst van 5G wordt het mobiele netwerk een steeds relevantere optie om breedbandige oplossingen aan te bieden. • Cloud based security • Service provisioning en automatisering • Block chain • Data science & analytics • Digitale data; Edge computing dataverwerking aan de rand van netwerken, vlakbij de bron van de data. • Ontwikkelingen op het gebied van security zoals: beter perfoance op versleutelde verbindingen in chip oplossingen, sleutelbeheer en authenticatie. • Het aantal SD-WAN software vendoren geleidelijk zal afnemen. Dat kan komen door consolidatie (overnames) of door het feit dat sommigen het eenvoudigweg niet gaan redden (beperkte schaalgrootte). De vendoren die overblijven zullen waarschijnlijk die partijen zijn met een grote footprint in de Telco en Service Provider markt.
		<u>Uitfaseringen:</u> • Een aantal technieken staan al langer op de nominatie om tot uitfaseren over te gaan. In de aankomende periode is het zeker dan ISDN en analoge verbindingen, Digistream en City Premium Access (CPA) voor een groot deel vervangen moeten gaan worden. In veel gevallen zijn er goede alternatieven beschikbaar maar zien wij eindgebruikers maar mondjesmaat voorbereiding te treffen voor deze uitfasering. Na de uitfasering van bovengenoemde technieken zullen ADSL en SDSL in rapper tempo minder relevant worden. • Legacy technologiën zoals SDH zullen vervangen worden naar meer schaalbare protocollen • Reguliere koperverbindingen t.g.v. de steeds hogere bandbreedte eisen • Lokale opslag verschuift naar cloudomgevingen • Traditionele firewalls worden vervangen door flexibelere systemen
B.5	Welke invloed gaat Software Defined Networking hebben op de interface tussen klant en service provider en op de dienstverlening van de service provider?	• De huidige rolverdeling tussen MJenV en opdrachtnemer zal veranderen. We gaan naar een automated netwerkomgeving toe waarbij in de meeste gevallen geen handmatige interactie met het netwerk meer noodzakelijk is. MJenV krijgt daarnaast meer en meer inzicht in en controle over de werking van het netwerk. Tevens is een betere sturing op end-to-end services mogelijk. • Het voordeel van SDN is de flexibiliteit t.a.v. implementatietijden. Vrijwel alle toe te voegen modules hebben een korte implementatie- en doorloop tijd doordat er geen hardware vervanging noodzakelijk is. Het betreft slechts een software module (licentie) dat aan de bestaande hardware wordt toegevoegd. • De invloed van SDN op dienstverlening: □ Verhoging van de operationele efficiency (up-/downscalen, automatisering van taken etc.) □ Verhoging van de operationele wendbaarheid (korte time to market) □ Pay as you use.

2 Informatie

Nr	Vraag	Antwoord
B.6	Hoe ontwikkelt Software Defined Networking zich in hun domein ook op de hogere lagen van dienstverlening (OSI-model)?	• Een deel van de partijen beperkt haar dienstverlening tot en met laag 3 (netwerk laag) van het OSI-model. De hogere lagen (4 t/m 7) uit het OSI-model vallen buiten de scope van hun dienstverlening. • De ontwikkeling zal zich concentreren op netwerk-aware applicaties. Deze applicaties zijn bijvoorbeeld instaat om meer of minder bandbreedte te vragen, Quality-of-Service aan te passen en problemen in het netwerk te detecteren etc. • Integratie met Virtuele netwerkfuncties (VNF) en Virtuele Security Functies (VSF) biedt mogelijkheden voor bijvoorbeeld een virtuele firewall. In plaats van de huidige (hardware matige) firewall oplossingen zijn deze straks eenvoudig op afstand te realiseren en te beheren in een virtuele omgeving.
B.7	Wat is de impact op de security functie van het netwerk in relatie tot koppelingen naar Cloudleveranciers?	• Beschikbaarheid wordt negatief beïnvloed door bijvoorbeeld DDoS attacks. Om deze DDoS attacks te vermijden of de impact ervan te minimaliseren kunnen er privé koppelingen gemaakt worden met de verschillende cloud-partijen. Daarbij helpt een DDoS mitigation service om het effect van een DDoS attack te minimaliseren. • Om vertrouwelijkheid en integriteit te bewaken is encryptie tussen klant en cloud essentieel (encryptie kan op applicatie- of op netwerkniveau plaatsvinden, of met virtuele cryptografie oplossingen). Daarnaast moet op de koppelvlakken een strikte security policy geïmplementeerd worden (bijvoorbeeld met FWs, IPS, IDS). Deze moet centraal aangestuurd worden en volledig geautomatiseerd doorgevoerd worden om menselijke fouten zo veel mogelijk te voorkomen, en consistentie en continuïteit van de dienstverlening te bewaken. • Het netwerk, de verkeersstromen en de ketens zijn te segmenteren, organisatorisch of op basis van het classificatie niveau van de uit te wisselen data. Deze verkeerstromen en segmenten zijn te koppelen op een of meer Public Cloud Providers, of externe netwerken die horen bij het classificatieniveau van de verkeerstromen. • Vanuit het netwerkstandpunt is een veilig koppelvlak aan te raden per Publieke Cloud Provider. Als veilig koppelvlak met een Public Cloud Provider is een (virtuele) Firewall in te zetten, waarmee een of meerdere geclassificeerde verkeerstromen zijn te koppelen met een of meerdere veiligheidszones/toepassingen van de Public Cloud Provider. • Binnen het netwerk het verkeer te controleren en desgewenst te filteren op verdachte informatiestromen. Hiernaast zijn (virtual) threat prevention toepassingen in te zetten op de koppelvlakken van het netwerk, om de justitie omgeving te beschermen tegen bedreigingen van buitenaf. Security en Compliance Monitoring de mogelijkheid om het geheel van eventuele verstoringen en verdachte gebeurtenissen of verkeersstromen in het netwerk in kaart te brengen en mitigerende acties te ontplooien. • Indien er gekozen wordt voor een privé koppeling zoals een IP VPN (MPLS) of een point-to-point connectie, dan hoeven er geen additionele securitymaatregelen getroffen te worden: private blijft private. Als daarentegen wordt gekozen voor een publieke koppeling (over het Internet) zal er rekening gehouden moeten worden met encryptie tunnels (SSL of IP Sec) en eventuele andere bijkomende beveiligingsmaatregelen. • In het geval van Over-The-Top (OTT) diensten hebben operators niet altijd zelf niet in de hand. Op dat moment wordt een vorm van "Edgde security" worden toegepast.
B.8	Hoe worden diensten als CASB (Cloud Access Security Broker) in de netwerkpropositie vormgegeven?	• Cloud Access Security Brokers (CASB's) zijn on-premise of cloud-based devices, geplaatst tussen cloud afnemers en cloud serviceproviders om beveiligingsbeleid van bedrijven aan te laten sluiten op de cloud. CASB's hanteren meerdere security policies. • Diensten zoals CASB zitten erg dicht op de eindgebruiker. Dit is een gebied waar traditionele service providers niet actief zijn. • Voor SD WAN gebaseerde netwerken, met toegang tot het internet, zullen security modulen in het netwerk apparaat (CPE) moeten worden opgenomen. Bedrijven leggen hun eigen richtlijnen vast in policies die door Secure Cloud Gateways worden van de leverancier worden afgedwongen. • Er zijn verschillende opties waar de CASB kan worden geplaatst: 1. Bij de Public Cloud Providers en externe koppelvlakken; 2. Decentraal op locatie van MJenV; 3. Via een centraal koppelvlak met het netwerk waar de CSP’s aan te koppelen zijn; Leveranciers hebben de voorkeur voor optie 3, deze is onafhankelijk van de cloudprovider.
B.9	Zijn er andere netwerk ontwikkelingen die de komende jaren van belang zijn voor JustitienNet4 en MinJenV?	• Zie ook B.1 en B.4 • Aan networking gerelateerde ontwikkelingen zullen ook de rol van netwerken beïnvloeden. Robotics, IoT, artificial intelligence, augmented reality, virtual reality, gamification, blockchain, quantum computing, big data analytics, videostreaming en 3D-printing zijn allemaal nieuwe toepassingen die gebruik maken van netwerken. Al deze ontwikkelingen betekenen dat er meer gevraagd gaat worden van netwerken op het gebied van bandbreedte, snelheid, automation, sturing en security.
B.10	In de netwerk wereld wordt al ca. 20 jaar gebruik gemaakt van protocollen zoals OSPF, IS-IS, MPLS, BGP4. - Van welke beperkingen in deze protocollen zullen we de komende jaren last krijgen.	• De antwoorden van de verschillende partijen over MPLS lopen uiteen: □ De protocollen zullen naar alle waarschijnlijkheid nog blijven bestaan. De protocollen hebben weinig beperkingen en ze zijn aanpasbaar om technologietrends te volgen, dat is ook de reden dat ze al zolang bestaan. □ De meeste ‘oude’ protocollen zijn te generiek. SDN zal bepaalde functies van deze protocollen overnemen, bijvoorbeeld om applicatiespecifiek verkeer te routeren. □ De komst van SDN zal hierin weinig veranderen, naarmate SDN complexer wordt zal deze technologie ook terugvallen op deze protocollen om het draaiend te houden. □ De beperking van het blijven gebruiken van legacy routeringsprotocollen zoals OSPF, IS-IS, MPLS en BGP is, dat er nauwelijks innovatie mogelijk is. • Het grootste zorgpunt is (op dit moment al) de hoeveelheid vrije IP-adressen op IPv4/ BGP4. Door o.a. de snelle ontwikkeling van IoT is er nu al behoefte aan meer IP-adressen. • Ethernet en IP zullen blijven bestaan. Dit betekent dat de impact op netwerken bij een uitfasering van sommige van bovenstaande protocollen beperkt is, waarbij sprake zal zijn van een geleidelijke transitie naar de logische opvolger.

2 Informatie

Nr	Vraag	Antwoord
B.11	Groei van bandbreedte is een van de belangrijke aandachtspunten van de afgelopen jaren geweest en schaalbaarheid van bandbreedte is een belangrijk aandachtspunt. De grote vraag is of de bandbreedte blijft groeien zoals de afgelopen jaren, of gaat de groei afvlakken of zelfs versnellen. Is er mogelijk een natuurlijk plafond, of niet. Hoe ziet de leverancier dit?	• Bandbreedte verdubbeling (wet van Moore) lijkt op een trend in de markt en deze trend lijkt niet te stoppen • Oorzaken nieuwe ontwikkelingen op het gebied van Mobility (5G), IoT, Video, Big data, shift to the cloud, smart city, smart car, Augmented Reality en Virtual Reality. • In theorie is er een natuurlijk plafond, in de praktijk zullen we daar echter niet aan komen. Bovendien zien we dat er steeds nieuwe ontwikkelingen ontstaan die de mogelijkheden voor bandbreedte verder oprekken. • De gebruikte crypto apparatuur moet kunnen meegroeien/voldoen aan deze groeiende behoefte.
C.	**Verkaveling**	
	Achtergrond C.1. t/m C.4.: **RWS CIV wil de mogelijkheden verkennen om de verkaveling toe te passen**	
C.1	Welke visie heeft leverancier m.b.t. een indeling van de diensten in percelen?	• Algemeen beeld is dat de grotere partijen voorstellen om vaste data OSI laag 1 t/m 3 in één kavel onder te brengen. • Één leverancier heeft de voorkeur om te verkavelen op basis van infrastructuur en diensten. • partijen die zich met name richten op security adviseren aparte kavels voor connectiviteit en security
C.2	Welke voor- en nadelen ziet de leverancier bij deze door hem voorgestelde perceelindeling	Voordelen van verkaveling infrastructuur en diensten: • Kavel voor infrastructuur kan voor een langere periode gecontracteerd worden. Daarbij wordt de mogelijkheid gecreerd om makkelijker, sneller en goedkoper te wisselen tussen de partijen op de hogere OSI lagen. • Komt de scheiding op zowel infrastructuur als op diensten ten goede. • Gebruik maken van bestaande netwerken om deze op te nemen in de bouw van het ondersteunende netwerk. • De partijen die een specifieke specialisatie hebben zich daarop kunnen onderscheiden. Voordelen van verkaveling connectiviteitsdiensten en security: • Onafhankelijke levenscycli van connectiviteit (zwarte netwerk) en beveiliging (rode netwerk). • Betere marktwerking doordat partijen niet van alle onderdelen expertise hoeven te hebben. • Verlaging van lifecycle kosten door connectiviteit en security te scheiden. • De partijen die een specifieke specialisatie hebben zich daarop kunnen onderscheiden. Voordeel van verschillende kavels voor vast en mobiel: • De partijen die een specifieke specialisatie hebben zich daarop kunnen onderscheiden. Voordelen van één perceel: • Ontzorgen, één aanspreekpunt en één dienstverlener • End-to-end verantwoordelijkheid, voorkomt fingerpointen tussen partijen • Minder beheerlast voor MJenV (minder partijen om te managen) • Minder complexe governance • Kortere oplostijden (minder partijen betrokken en duidelijke probleemeigenaar) Standpunten over kostenvoordeel bij meerdere kavels lopen uiteen.
C.3	Wat is de visie op de integratie van netwerk en security?	• Het netwerk en de security van het netwerk niet los van elkaar gezien kunnen worden en vragen om een integrale aanpak. • De basis is en blijft de komende jaren een netwerkinfrastructuur met een basis security schil, zoals lijnbeveiliging. Op deze basisinfrastructuur kunnen verschillende security bouwblokken worden ingepast. Denk hierbij aan toekomstscenario's waarbij SDN en cloudtoepassingen gaan vragen om specifieke beveiligingsoplossingen (bijvoorbeeld een securitybeweging naar de 'edge'). • De argumenten om netwerk en security te integreren zijn: □ Om een robuust en veilig netwerk te leveren. □ Verkeer tussen diverse klant-groepen veilig van elkaar te kunnen scheiden. □ De justitieomgeving te beschermen tegen security risico's op netwerkniveau en vanuit koppelvlakken, aan te sluiten netwerken. □ Het bijdragen aan en het borgen van de vertrouwelijkheid en integriteit van de justitie omgeving is alleen mogelijk door het leveren van een netwerk, geïntegreerd met security toepassingen.
C.4	Mobiele datanetwerken (3G, 4G, 5G, wifi) en de vaste datanetwerken worden nu veelal los van elkaar georganiseerd en kennen veelal verschillende, standaardisatiefora, leveranciers, contracten etc. Zijn hier de komende jaren integraties te verwachten, welke?	• Niet alle geconsulteerde partijen leveren zelf Mobiele netwerken. • Mobiele netwerken kunnen eenvoudig kunnen geïntegreerd worden als een access technologie voor IPVPN netwerken. • In de toekomst zal 5G naar een hogere bandbreedte ook gaan leiden tot een lagere latency en door middel van network slicing zullen er ook garanties kunnen worden afgegeven. • Er wordt een volledige ontkoppeling van de access (zowel fixed als mobiel) en de aangeboden diensten voorzien. Hierdoor wordt het mogelijk om elke dienst te leveren over elke access methode. • Veel nieuwe mobiele devices en Internet of Things (IoT) toepassingen maken al gebruik van mobiele datanetwerken en zullen dat in toenemende mate gaan doen. • Netwerken zullen in de toekomst bestaan uit een mix van mobiele en vaste netwerken en als één geheel acteren. Belangrijk is wel een centrale security laag, aangevuld met encryptie en end-point protectie.
D	**Migratie**	

2 Informatie

Nr	Vraag	Antwoord
	Achtergrond D.1. RWS CIV hecht er een groot belang aan migraties tussen latende naar de nieuwe leveranciers probleemloos en volgens planning verlopen.	
D.1	Welke visie heeft de leverancier hoe de migratie JN3 -> JN4 zou kunnen worden georganiseerd en uitgevoerd zodat een zo soepel en snel mogelijke migratie kan worden gerealiseerd?	• De beantwoording van de vraag tussen de verschillende leveranciers loopt zeer sterk uiteen in diepgang en aanpak. Het is de verwachting dat deze vraag een andere vorm terugkomt in het vervolg van de aanbesteding. Hierdoor is sprake van commercieel vertrouwelijke informatie en dit is de reden dat er geen details van de strategieën van de verschillende leveranciers in dit document vermeld. • Het gezamenlijk organiseren en voorbereiden van een migratie is een essentieel onderdeel in de project aanpak. Door in de beginfase heldere en realistische doelstellingen gezamenlijk te formuleren en de daarbij behorende voorbereidende werkzaamheden goed op elkaar af te stemmen zorgt ervoor dat op een soepele migratie mogelijk is, ook in complexe migratieprojecten.
E.	**Kwaliteitsmanagementsysteem, Kwaliteit en Kennis**	
	Achtergrond E.1. t/m E.2.: RWS CIV hecht er een groot belang aan dat leveranciers de gevraagde dienstverlening onder kwaliteitsborging uitvoeren. RWS CIV is benieuwd op welke wijze de kwaliteit door leveranciers wordt geborgd.	
E.1	Welke kansen en risico’s ziet u als Marktpartij?	<u>Kansen:</u> • Leverancier specifieke kansen zijn niet in dit document opgenomen vanuit concurentieperspectief. • In de huidige aanbestedingen wordt kwaliteit opgelegd door standaarden en scherpe boete clausules. Dit staat naar onze mening haaks op het gezamenlijke belang om dienstverlening te verbeteren. In een optimale wereld zijn huidige vormen van kwaliteitsborging (ISO, BIR etc) de basis om te starten. De overeenkomst moet daarna mogelijkheden bieden om af te wijken van de standaarden en voorwaarden om te komen tot een betere invulling voor beide partijen. • Mogelijkheid om naast de realisatie van de harde servicelevels ook naar de klanttevredenheid van de dienstverlening mee te nemen. <u>Risico:</u> • Indien RWS CIV en MJenV besluiten om een niet-marktconforme vereiste uit te vragen waarop marktpartijen niet op tijd kunnen reageren, dan is dat een groot risico. De huidige elementen voor kwaliteitsborging en opvolging meer dan voldoende. • Weging kwaliteit en governance in de aanbesteding: het risico is dat de focus in de aanbesteding vooral komt te liggen op contractuele eisen, harde KPI´s en een lage prijs. Het advies is daarom om in de aanbesteding voldoende ruimte te bieden voor een open beantwoording ten behoeve van kwaliteit (soft KPI’s zoals empathie, communicatie en betrokkenheid) en governance. • De afhankelijkheid van de kwaliteit en continuïteit in de keten. De hele keten dient eenzelfde kwaliteitsbewustzijn en borging na te streven met eenzelfde mate van volwassenheid en de verschillende inspanningen en systemen dienen op elkaar afgestemd te worden. het bewustzijn van alle stakeholders speelt hierbij een hele belangrijke rol.
E.2	Welke kansen en risico’s ziet u voor RWS CIV en MJenV?	<u>Kansen:</u> • MJenV zal profiteren van een stabiele leverancier voor WAN diensten zoals IP VPN, Ethernet VPN, Ethernet P-2-P connecties, Cloud Access, Data center- en Internet diensten. • Mogelijkheid om naast de realisatie van de harde servicelevels ook naar de klanttevredenheid van de dienstverlening mee te nemen. • Openheid in architectuur: een kans om transparant te zijn over de gewenste netwerkarchitectuur en het beleid eromheen. Door hier open over te communiceren kunnen marktpartijen beter inspelen en hun roadmap beter afstemmen op de (toekomstige) wensen van MJenV. Daarnaast kan er meegedacht worden over de optimale invulling van bepaalde wensen en eisen met betrekking tot architectuur, en hoe hier zo efficiënt en effectief mogelijk mee omgegaan kan worden. • Vragen naar onderscheidend vermogen van de aanbieders. Wat kunnen de aanbieders extra bieden ten opzichte van de standaarden om de kwaliteit te borgen en te verbeteren in samenwerking met MJenV. • Het is voor opdrachtnemers erg belangrijk om duidelijkheid en voorspelbaarheid te hebben in de forecast van af te nemen diensten. MJenV zou de aanbesteding kunnen gebruiken om deze duidelijkheid en voorspelbaarheid te vergroten door deze achtergrondinformatie op te nemen in de uitvraag, zodat de opdrachtnemer beter in kan spelen op de aanstaande behoeftes. • De kans om de eisen en wensen op het gebied van kwaliteitsmanagement aan te scherpen en met name te kijken naar de mate waarin leveranciers met dit kwaliteitssysteem ook daadwerkelijk de gewenste kwaliteit leveren in termen van betrouwbaarheid en veiligheid (prestatie-informatie) en bereid zijn daarover garanties te geven. • De partijen die een specifieke specialisatie hebben zich daarop kunnen onderscheiden. • Borging van de kwaliteit van de lijnbeveiligingsproducten door NBV erkende producten te eisen.

2 Informatie

Nr	Vraag	Antwoord
		Risico: • Het afdwingen van randvoorwaardelijke eisen in de aanbesteding is zeker geen garantie voor kwaliteit. Immers op deze wijze zal de kwaliteit nooit groeien. De noodzakelijke inspanning zal geleverd moeten worden om aan alle eisen van deze dwangbuis te voldoen. RWS CIV en MJenV kunnen zich beter richten op de uitvraag op basis van de bestaande kwaliteits-borgingen in Europese Aanbestedingen en samen met de gegunde partij werken aan het gezamenlijke belang om de kwaliteit te verhogen. • Weging kwaliteit en governance in de aanbesteding: Dit betreft een gedeeld risico • Openheid over architectuur: het als een risico voor MJenV indien besloten wordt geen openheid te geven over de gewenste netwerkarchitectuur en het beleid eromheen. • Het is een risico voor MJenV dat opdrachtnemers zich zeer rigide opstellen en contracten en SLA's naar de letter van de wet invullen. Hierdoor wordt de flexibiliteit beperkt. RWS CIV en MJenV zouden er goed aan doen om bijvoorbeeld geen maximale doorlooptijden op incidenten te definiëren, maar een maximale beschikbaarheid. Zodoende hoeft de opdrachtgever geen genoegen te nemen met maximale oplostijden en kan de opdrachtnemer zich hier niet achter verschuilen. • Het risico bestaat dat een aanbieder op papier wel een kwaliteitssysteem heeft, maar dat dit in praktijk niet bijdraagt aan een hogere kwaliteit van de geleverde dienst. Het kwaliteitssysteem en de geleverde prestaties zullen continue beoordeeld moeten worden.
F.	**Overig**	• Meerdere partijen hebben gevraagd om eventuele roadmap van MJenV in de aanbesteding te delen. • Neem de waardering voor een degelijk governance model uit te drukken in duidelijke wegingsfactoren tijdens de aanbesteding. • Klimaat en duurzaamheidsdoelstellingen en hergebruik middelen. • Ruimte voor innovatie en toevoeging van nieuwe diensten tijdens de contractduur. • Maak het prijsmodel niet onnodig complex. Beperk de opties.
G.	**Interviews**	SDN: • SDN is nog volop in ontwikkeling. Daarom SDN is wel een vernieuwing die gaat spelen gedurende de voorziene looptijd van het contract. Er dient voldoende contractuele ruimte zijn voor de partijen om deze nieuwe ontwikkelingen te kunnen adopteren. • SDN biedt eenvoud in uitrollen, snelheid van changes, on-demand bandbreedte en het softwarematig inschakelen van netwerk functies (NFV) op klantlocaties zijn vanuit de klant gezien extra functies. • De grootste voordelen van SDN liggen bij de netwerkpartijen. • De voordelen voor de klant liggen voornamelijk op het gebied van flexibiliteit en snel (on-demand) kunnen schalen. Echter dit voordeel valt weg indien er nieuwe of andere fysieke verbindingen moeten worden aangelegd. • Daarnaast is een toepassing het off-loaden naar Internet via een local breakout om daarmee de kosten te reduceren. Dit kan zijn voor minder kritisch verkeer, of verkeer naar public cloud diensten, of het gebruik van Internet als backup als de MPLS lijn niet functioneert. • De providers staan aan het begin van een ontwikkeling, enkele hebben functionerende diensten. Er is nog geen sprake van vervanging van de MPLS diensten maar een aanvulling op. • Enkele partijen voorzien dat de CPE geen netwerkdevice maar een generiek CPU platform wordt, waarop netwerk functies kunnen draaien. Er wordt ook overwogen wordt software van derden op het platform te laten draaien. Een nog niet opgelost vraagstuk hierbij was beheer en demarcatie van beheer domeinen.
		<u>5G:</u> • De eerste introductie van 5G zal nog enkele jaren duren (2020). Uitrol begint in de steden. Veel van de partijen zijn op dit moment nog 4G aan het uitrollen. • Voor landelijke uitrol zullen eerst de licenties geveild moeten worden, vervolgens kunnen service providers hun netwerk gaan bouwen. Verwachting is dat landelijke uitrol enkele jaren (3-5) gaat duren voordat 5G landelijk in voldoende capaciteit beschikbaar is. Al met al is de verwachting dat 5G pas over meer dan 5 jaar relevant kan zijn voor JN4. • De toename aan IOT-oplossingen is een van de drijvende krachten achter 5G. • Extra mogelijkheden: vervanging van Wifi, vervanging vaste verbindingen, redundantie, snel uitrollen extra capaciteit.
		Cloudconnecties: • Alle service providers bieden mogelijkheden om directe verbindingen naar de grote cloud providers (MS, Google, AWS) te realiseren. • De Equinix Cloud Exchange is door meerder partijen genoemd als mogelijkheid om ook direct naar de minder grote partijen te koppelen. • SDN functies kunnen worden gebruikt om zeer flexibel bandbreedte te kunnen schakelen naar cloud partijen. • End-to-End netwerk encryptie tot en met de systemen bij cloud providers is technisch mogelijk, doordat SD-WAN/crypto devices op virtuele hardware kunnen draaien. In dienstverlening zijn er nog beheer(domein) vraagstukken.
		Verkaveling: • Het grootste deel van de partijen ziet een traditionele verkaveling voor zich, waarbij laag1 t/m 3 en de security in één perceel is ondergebracht. • Een partij ziet ook mogelijkheden om laag1 (evt. in combinatie met laag2) in een apart perceel onder te brengen. In deze lagen gaat het voornamelijk om bandbreedte en fysieke infrastructuur. Door hiervoor langjarige contracten af te sluiten kan Justitie zorgen dat op alle (strategische) Justitie locaties glasvezel beschikbaar komt. Deze laag kan vervolgens door andere partijen gebruikt worden om diensten te leveren. Deze diensten kunnen in andere percelen worden ondergebracht, zoals van bijvoorbeeld een perceel voor een Laag3 (IP VPN) en security dienst. • Enkele partijen zien beveiliging mogelijk als een apart perceel.

2 Informatie

Nr	Vraag	Antwoord
		Security: • Security is met de cloud ontwikkeling steeds lastiger te scheiden of te concentreren in een centrale functie. Enkele netwerkpartijen geven aan dat security weer een groter aandachtsgebied wordt. • Security verschuift naar de randen van het netwerk. • Crypto dienstverlening is standaard onderdeel van SD-WAN oplossingen. Deze zijn veelal gebaseerd op Ipsec (encrypted tunnels), of Ipsec maakt onderdeel uit van SD-WAN diensten. • IP VPN dienstverlening is ook mogelijk op basis van OpenVPN-NL encrypte tunnels. • Belangrijke eis: de snelheid van doorvoeren van security patches op de infrastructuur & gezamenlijke overweging integriteit/confidentialiteit vs. beschikbaarheid. • In hoeverre wil je met de cryptolaag ook metadata verhullen (wie zet een VPN verbinding op met wie, wie wisselt verkeer uit met wie?). • Asymmetrische encryptie/PKI is de onderhandeling en het opzetten van de encryptie/tunnel het zwakke punt. Nieuwe versie van TLS1.3 en OpenVPN-NL verbeteren dit door de onderhandeling te encrypten. • Generiek gesproken is symmetrische encryptie beter bestand tegen de gevaren van het post quantum computing tijdperk.
		<u>Infrastructuur:</u> • De capaciteit van Coax netwerken wordt met de uitrol van docsis3.1 hoger. Snelheden van meer dan 1Gbps zijn mogelijk. Op coax is geen QoS mogelijk en wordt overbooking toegepast. Deze netwerken hebben een hoge dekkingsgraad. • Met de ontwikkeling van 5G zal er volgens partijen meer behoefte komen aan glasvezel in buitengebieden. • Er zijn mogelijkheden om de investeringen in glas, die de afgelopen contract periode door Justitie zijn gedaan, in te brengen in een nieuw contract. Het zal afhangen van de specifieke situaties en omvang van het glasvezelproject. • Eén grote glasvezel businesscase kan aantrekkelijk zijn voor providers: □ Dure locaties (veel graven) compenseren met goedkope locaties (al of bijna on-net) □ Ze breiden hiermee hun netwerk uit in buitengebieden • Investeren in glas biedt Justitie de mogelijkheid van bandbreedte beperkingen (koperlijnen en straalverbindingen) af te komen & is toekomstvast. • Elkaars netwerk gebruiken (wholesale) wordt in de toekomst met SDN makkelijker, hiermee kunnen providers geautomatiseerd circuits op elkaars netwerk bestellen en realiseren. Enkele partijen hebben dit al ingericht. • Overweeg of anti-DDoS niet aan de scope toegevoegd moet worden. Er is dan sprake van van DDoS geschoond internet. Dit wordt in al het netwerk van de partij opgevangen i.p.v. binnen het netwerk van MJenV.
		<u>Kwaliteit:</u> • Klanttevredenheid / continious improvement, hoe te voorkomen dat gewenste antwoorden worden gegeven, en er in de praktijk niet veel van terecht komt? • Wil je als klant flexibiliteit, doe dan ook aan prioriteitsstelling.
		<u>Bandbreedte & pricingmodellen:</u> • Met SDN is een trend naar flexibilisering van bandbreedte zichtbaar. Enkele providers spreken hier over "Bandbreedte on demand" en "Pay as use". • Klanten kunnen middels Portals zelf bandbreedte aanvragen, middels API's zou dit ook geautomatiseerd kunnen worden. Mogelijk gaan applicaties directe bandbreedte vragen. • Aangegeven wordt dat volledig "Pay as use" komende 3-4 jaar nog niet te verwachten is. De netwerken zijn hier nog niet op ingericht. • Zijn we niet teveel aan het micromanagen op bandbreedte? • Kan facturatie eenvoudiger door bijv. 2 keer per jaar bepalen wat de kosten zijn? • De basis glasvezel infrastructuur die providers neerleggen naar een locatie heeft een capaciteit van 1G of 10G (of meer). Vervolgens wordt dit "geknepen" naar de afgenomen bandbreedte. Met dit gegeven zouden de kosten van een "flat fee" model, met als standaard bandbreedte 1G of 10G lager kunnen zijn dan een "geknepen" model. Immers de investeringen blijven hetzelfde, maar beheerkosten (upgrades/downgrades/facturatie) nemen af. • Twee providers hebben aangeven dat een "flat fee" model een reële optie is.
		Suggesties aanbesteding / contract:: • Creëer voldoende ruimte in het contract om nieuwe ontwikkelingen en veranderingen (technologie, samenwerkingsvormen, governance etc.) te kunnen adopteren. • Creëer voldoende ruimte in het contract om indien noodzakelijk (bijvoorbeeld een heel lastig te ontsluiten locatie) ook alternatieven in te zetten die indien ze door de klant geaccepteerd worden aan minder stringente eisen hoeven te voldoen. • Maak de periode van verlengingen niet te kort. Dit geeft onvoldoende ruimte aan de partijen om nog vernieuwingen door te voeren. • Marktconformiteitstoetsen leveren in de praktijk vaak discussies op. Denk na of er niet beter met verlengingen gewerkt kan worden om de prijs marktconform te houden. • Deel de besparingen van innovaties/besparingen tussen klant en marktpartij. Dit stimuleert de partijen meer om hierin te investeren. • Hoe geven we partijen voldoende ruimte om te doen waar ze goed in zijn? In een strak en vooral op prijs gebaseerd contract is hier geen ruimte voor. Een innovatiepot is een mogelijke maatregel om gedurende het contract geld te investeren in innovatie. • Wat zijn de gevolgen voor aangeboden diensten als door de Brexit als de UK opeens geen onderdeel van de EU meer is. • Er wordt speciale aandacht gevraagd voor het borgen van het level playing field. • Het is een optie de partijen in de aanbesteding een visie geven op preventieve, detectieve en correctieve beveiliging. • Hou de aanbesteding vooral functioneel (het wat en niet het hoe)