

Samenvatting Consultatie-antwoorden via TenderNed
IUC-EZK, IWR
10 maart 2023

Inleiding

Dit document bevat de vragen die in de context van de marktraadpleging IWR 2024 Vaste Telefonie (TenderNed kenmerk 389163) op 18 december 2022 aan de markt zijn voorgelegd, Per vraag zijn daarbij de van vier respondenten ontvangen antwoorden opgenomen. Waar nodig geacht zijn teksten door IWR geanonimiseerd of ingekort. Daarbij is de verwijzing naar Partij 1, 2, 3 en 4 bij alle vragen steeds dezelfde. Dit document wordt via de TenderNed-consultatie gepubliceerd.

Vraag en antwoord

Nr	Vraag
1a	Wat is uw zienswijze met betrekking tot PSTN - ontsluiting voor cloud (SaaS) gebaseerde telefonie oplossingen zoals bijvoorbeeld Microsoft Teams Voice, Webex Calling en Webex Contact Center?
Partij 1: Twee mogelijkheden: 1. Ontsluiting via "infrastructure as a service" en aansluiting op een SaaS-platform; 2. Aansluiting op een SaaS platform via een SIP trunk. Partij 2: De kern van de vaste telefoniedienst bestaat uit het leveren van spraakdiensten over een Voice-over-IP-verbinding (VoIP). Hiermee is bellen over het internet via een eigen telefooncentrale op locatie of een telefooncentrale uit de cloud zoals Microsoft Teams mogelijk. Ontsluiting van diensten via Internet of via VPN. Partij 3: We zien in de markt toenemend hybride gebruik van (cloud)PBX en Unified Communications oplossingen als Teams en Webex. Een volledige overstap naar UC zien we nog nauwelijks, ook uit proof of concept testen is vaak het resultaat dat er geen volledige overstap van PBX naar UC voor individuele telefonie plaatsvindt. Inschrijver ziet Teams als een waardevolle aanvulling op de telefonieomgeving, echter wordt Teams ingezet als middel om geplande vergaderingen te houden. Telefonie voor deelnemers met hoog volume telefonieverkeer worden te allen tijde ingericht met een dedicated omgeving voor bereikbaarheid. Derhalve ziet inschrijver SaaS oplossingen zoals Teams en Webex los van het perceel vaste telefonie. Callcenter functionaliteit wordt niet of nauwelijks gemigreerd naar UC. We zien bij veel klanten PSTN lijnen termineren op een SBC, waar vervolgens een keuze gemaakt wordt om het betreffende nummer af te handelen op een contact center oplossing, op de traditionele PBX of op UC. Garanties op spraakqualiteit zijn voorbehouden aan PSTN lijnen op een PBX. Oplossingen over internet ofwel OTT (Over the Top)bieden vaak voldoende kwaliteit voor reasonable effort kwaliteit individuele gesprekken, maar geen garanties. Partij 4: Ons bedrijf levert een oplossing voor Microsoft Teams Phone ontsluiting, door Microsoft Direct Route genoemd. Bij de introductie van die dienst was Ons bedrijf Nederland uniek in Europa omdat wij PSTN als een cloud gebaseerde dienst leverden. Afgezien van het leuke feit dat Ons bedrijf als voorbeeld werd genoemd tijdens het Microsoft Ignite event en we hebben gesproken bij Audiocodes voor alle Europese partners heeft deze vroege introductie ons veel ervaring opgeleverd. Deze introductie past in de cloud visie van ons bedrijf op al haar diensten. Alle UC/CC gebaseerde diensten zijn inmiddels cloud gebaseerd, zo ook onze One Net dienst waar Webex een onderdeel van is. PSTN als onderdeel van een volledig gehoste UC/CC oplossing of als zelfstandige dienst past dus in onze visie op de toekomst.	

1b	Ziet u behalve de drie in vraag 1a gegeven voorbeelden andere SaaS-gebaseerde telefonieoplossingen in de markt in (opkomend) gebruik? Zo ja, welke?
	Partij 1: NEC met UNIVERGE BLUE Deze dienst biedt zowel IaaS, SaaS als CaaS en integreert met MS Teams op basis van cloud to cloud. Partij 2: SaaS-gebaseerde telefonieoplossingen: • Mitel- een Unified Communications IP-PBX oplossing met uitgebreide traditionele telefonie functionaliteiten. Gehost in het datacenter biedt deze vooral extra functionaliteit als er op een specifieke locatie een directe koppeling naar Zorg/IoT oplossing gewenst is; • Genesys Cloud- een All-in-One Omnichannel contactcenteroplossing voor optimaal routeren van alle type interacties zoals spraak, e-mail, web messaging en social mediakanalen. Onderscheidend met geïntegreerde recording en WorkForce Management (WFM) oplossing voor planning en roostering van medewerkers. Gehost in Amazon Web Services (AWS). • Anywhere365- uitgebreide contactcenterfunctionaliteiten en bedienpostoplossing voor recepties. Uitsluitend in combinatie met Microsoft Teams. Gehost in de Azure-Cloud. Partij 3: Ja, naast UC oplossingen zien we veel hosted telefonie. Daarbij geldt dat hosted telefonie superieur is in features en zeker in vast mobiel integratie. Operators bieden ook cloud SBC oplossingen als SaaS dienst, met daarachter de uitsplitsing naar verschillende toepassingen. Klanten waarbij telefonie belangrijk is voor het primaire bedrijfsproces maken nu en in de nabije toekomst gebruik van een PBX al dan niet cloud gebaseerd. Hierin zien we op korte termijn geen verandering. UC en vast-mobiel integratie worden daar vaak als add on op de PBX toegevoegd. Partij 4: Vrijwel iedere UC/CC partij heeft tegenwoordig een SaaS gebaseerde UC/CC oplossing. Dit zijn vaak zelf ontwikkelde oplossingen of een OEM versie. Hier is geen dominante partij in te onderscheiden anders dan Ringcentral dat voor vrijwel alle grote UC partijen de onderliggende leverancier is. Onder andere Alcatel-Lucent, Atos, Avaya, Mitel en onze dienst gebruiken Ringcentral voor hun SaaS UC oplossing.
2a	Welke standaard oplossingen kunnen er door u aangeboden worden om de SaaS omgevingen van PSTN connectiviteit te voorzien, zoals bijvoorbeeld voor direct "cloud - cloud"?
	Partij 1: PSTN ontsluiting geheel uit de cloud (siptrunk as a service) of Bring your own trunk waarbij de siptrunk van de klant via een SBC aangesloten wordt op de cloud omgeving. Partij 2: Twee soorten internetverbindingen om SaaS omgevingen van PSTN connectiviteit te voorzien: 1. Standaard internet (overbooked/gedeelde bandbreedte); 2. Premium internet waarbij gewenste bandbreedte gegarandeerd is en er hogere beschikbaarheid geboden kan worden door redundante apparatuur en separate glasverbindingen naar verschillende lokale PoP's (wijkcentrales). Om verschillende verkeersstromen (voice en data) te kunnen classificeren en prioriteren, is er de Software Defined-WAN dienstverlening bovenop de internet/VPN-laag. Een gesloten netwerk met gegarandeerde bandbreedte voor klantlocaties; Connectiviteit naar de buitenwereld/internet via een centrale firewall (managed dienstverlening inclusief flexibele bandbreedte). 1. Cloud Connect maakt het (cloud-cloud) mogelijk om vanuit het datacenter cloud diensten, te faciliteren (bijvoorbeeld Azure of AWS) 2. Elastic Interconnect: a. biedt volledig inzicht in internetconnectiviteit en voorziet uw organisatie van verbindingen van hoge kwaliteit en extreem lage latency; b. Deze verbindingen communiceren met Cloud Service Providers, Cloud Security

Brokers, SaaS-applicaties, Internet Service Providers en andere dienstverleners; c. via een besloten netwerk toegang tot uw klanteigen omgevingen in private clouds, zoals AWS en Azure. Real-time en historisch time inzicht in alle verbindingen. Mogelijkheid van doorvoeren van wijzigingen in het netwerk.

Partij 3: Indien garanties op telefonie gewenst zijn, worden OTT verbindingen uitgesloten. Veel SaaS providers zijn op ons netwerk ook beschikbaar om directe verbindingen mee te leggen. Met name in het hybride scenario dat voor veel overheidsinstellingen van toepassing zal zijn, lijkt een cloud SBC de meest geëigende oplossing.

Partij 4: Calling in Office365 is onze standaard dienst om Direct Routing te leveren voor Microsoft Phone. In deze oplossing leveren wij Audiocodes SBC functionaliteit gecombineerd met PSTN, security en technisch/operationeel beheer vanuit onze datacenters. Onze One Net propositie levert PSTN connectiviteit voor onze Webex propositie. Dit is een gecombineerde dienst waarbij we UC/CC functionaliteit, PSTN, security en technisch/operationeel beheer als complete SaaS dienst leveren. Onderdeel van die dienst is ook Webex. Daarnaast kunnen wij op verzoek SBC functionaliteit gecombineerd met PSTN, security en technisch/operationeel beheer leveren vanuit ons datacenter voor andere UC/CC platformen.

2b	Welke van de onder vraag 2a benoemde oplossingen heeft (hebben?) uw voorkeur voor toepassing in de rijksomgeving, en waarom?
-----------	---

Partij 1: Door de PSTN-ontsluiting geheel in eigen cloud-omgeving op te nemen is er geen infrastructuur aan de kant van de opdrachtgever nodig en wordt – bij trunks zonder redundancy - een single point of failure vermeden.

Partij 2: Op basis van specifieke eisen en wensen op het gebied van beschikbaarheid, security en budget kan in overleg de best passende propositie worden gemaakt uit de onder 2a benoemde connectiviteit portfolio.

Partij 3: Cloud SBC, al dan niet voorzien van (cloud) PBX en direct route naar UC toepassingen.

Partij 4: Microsoft Teams is op dit moment dominant in bij overheid en bedrijfsleven als UC oplossing. Nog niet qua installed base maar wel als het platform waar bedrijfsleven en overheden naar overstappen. Ons bedrijf is heel sterk in die markt en heeft dus veel ervaring met de toepassing van Microsoft Teams in zowel de publieke sector maar zeker ook in de private sector. Uit die ervaring zijn 2 dominante lessen te trekken: Microsoft Teams is geen complete UC oplossing en zeker geen CC oplossing. Het moet dus altijd aangevuld moeten worden met externe applicaties voor geavanceerde UC functionaliteit, zoals rapportages en bedienpostfunctionaliteit en voor CC functionaliteit die verder gaat dan huntgroepen. De hiervoor benodigde integraties zijn in de praktijk minder functioneel en gebruiksvriendelijk door beperkingen die Microsoft heeft in de GraphAPI. De share of wallet voor UC/CC partijen bij een Microsoft implementatie is significant lager dan bij een voorheen gebruikelijke UC/CC verkoop. Dit is het resultaat van diverse directe afspraken tussen de overheid en Microsoft, zoals de Rijksbrede Microsoft Business and Services Agreement. Dit drukt op de business case, waardoor grote aanbestedingen in de publieke markt op minder enthousiasme kunnen rekenen dan voorheen. Dit feit, gecombineerd met de wens van aanbestedende partijen om de verantwoordelijkheid voor de totale dienst bij 1 partij te beleggen, zorgt voor terughoudendheid in de markt. Aanbestedende diensten realiseren zich onvoldoende dat ze geen UC oplossing meer aanbesteden, maar PSTN connectiviteit en aanvullende CC functionaliteit. Dit vertaalt zich in bestekken die uitgebreid ingaan op UC functionaliteit, die de inschrijvers feitelijk niet meer bieden, en SLA's die zien op de combinatie PSTN, UC en CC, terwijl inschrijvers die verantwoordelijkheid niet meer kunnen nemen. Vanuit een functioneel, financieel en ketenverantwoordelijk oogpunt heeft ons bedrijf dus een voorkeur voor een UCaaS en CCaaS oplossing boven Microsoft Teams.

3a	Vast-mobielintegratie is al enige tijd een hot topic in de markt. Zeker wanneer het ook oplossingen biedt als mobiel bellen met een vast nummer en uniforme beschikbaarheids-informatie delen (presence). Wat is uw zienswijze over een uniforme gebruikerservaring en (seamless/naadloze) bereikbaarheid, of men nu communiceert vanaf een vast toestel, een laptop, een tablet of een smartphone?
	Partij 1: In "Bereikbaarheid" bepaalt de gebruiker steeds meer zelf waar, wanneer en hoe hij bereikbaar is. Technologie dient ondersteunend te zijn. Door de gebruiker de mogelijkheid te geven van verschillende soorten devices (laptop, tablet, smartphone of vast toestel) en deze devices bereikbaar te maken onder 1 vast nummer verkrijgt de gebruiker de vrijheid om te kunnen communiceren op de manier zoals het hem of haar past. Door tijdens een gesprek heel makkelijk naar een ander device te switchen zonder dat dat impact heeft op de gesprekspartner wordt er nog meer gebruiksgemak gecreëerd. De presence van een gebruiker wordt gemonitord aan de status van zijn device(s), de status wordt vervolgens aan anderen inzichtelijk gemaakt in bijvoorbeeld het adresboek waarmee anderen weer de bereikbaarheid van de gebruiker inzichtelijk krijgen. Partij 2: Respondent ziet dat op kantoor en thuiswerken steeds meer door elkaar heen lopen en dat de medewerker steeds meer verwacht dat de bereikbaarheid optimaal is. Het toestel of netwerk mag hierin niet belemmerend werken. Ook respondent ondersteunt mobiel werken voor haar eigen medewerkers. Het wordt steeds belangrijker dat alle faciliteiten die men gewend is op de vaste werkplek naadloos overgaan naar het mobiele device, ongeacht of dit een laptop, een tablet of een smartphone betreft, of de medewerker nu op kantoor werkt, thuis of op reis is. Respondent verwerkt deze vervlechting van verschillende diensten en functionaliteiten ook in haar eigen portfolio. Belangrijk hierin is dat zowel vaste telefonie als mobiele telefonie bij Respondent worden afgenomen om te kunnen integreren. Partij 3: We bieden vast-mobiel integratie op onze SaaS telefonie oplossingen, én de mogelijkheid om vast-mobiel te integreren op uw eigen PBX, én de mogelijkheid om vast-mobiel te integreren op Teams. Inschrijver gelooft in gebruikersvriendelijkheid van de oplossingen, en vast-mobile integratie is hierin een belangrijke feature. Een volledige vast-mobiel integratie met alle functionaliteiten is pas mogelijk wanneer zowel mobiel als vast bij 1 provider zijn ondergebracht. Overige vast-mobiel integratie oplossingen die niet gebaseerd zijn op de native dialer van het mobiele toestel, worden door gebruikers als niet gebruikersvriendelijk ervaren. Partij 4: Voor ons bedrijf is het belangrijk dat iedereen altijd en overal kan werken op een manier die het beste bij hem/haar/het past. Vanuit die visie heeft ons bedrijf al jaren vast-mobiel oplossingen. Variërend van Corporate Net, Forced on PBX en twinning tot mobiele UC app's. Sinds een jaar hebben we daar echter ook een netwerk gebaseerde oplossing bij, Vast op Mobiel. Vanuit die oplossing kunnen wij de mobiele netwerk presence (bezet/vrij) op basis van een API delen met een UC/CC oplossing. Standaard doen we dat al met Microsoft Teams, maar andere platformen zijn met enig maatwerk ook mogelijk. Daarnaast kunnen gebruikers vanaf de native dialer van hun mobiel met een vast nummer uitbellen. De gebruiker kan zelf wisselen tussen het uitsturen van een vast of mobiel nummer. Voor gebruikers van tablets en laptops zijn App's en WebRTC gebaseerde oplossingen beschikbaar m een uniforme gebruikerservaring te ervaren.
3b	Wat is uw verwachting van de ontwikkelingen op het onder 3a genoemde gebied voor de komende jaren?
	Partij 1: We verwachten dat vast mobiel integratie steeds meer naar een app verschuift ipv vanuit de native dialer, waarbij GSM wordt gebruikt voor prive gesprekken en de app voor zakelijke gesprekken. Daarnaast zien we dat MS Teams steeds meer wordt opengesteld voor integratie op onder andere het gebied van presence, hierdoor kunnen verschillende communicatieplatformen op elkaar worden afgestemd en inzicht geven van elkaars beschikbaarheid.

Partij 2:

De verwachting voor de komende jaren is dat medewerkers steeds meer hybride gaan werken, zowel op kantoor, thuis of elders. Vast-mobielintegratie wordt steeds belangrijker, waarbij de overgang van vast naar mobiel werken naadloos moet zijn en geen nadelen moet opleveren in de bereikbaarheid. Presence, meetings en het zelfstandig beheren van je bereikbaarheidsprofiel wordt daarin steeds belangrijker. Het mobiele device heeft steeds meer toegang tot vertrouwelijke bedrijfsgegevens en daarbij staat de medewerker en het bedrijf steeds meer blootgesteld aan bedreigingen van virussen en malware. Security ook op de mobiele devices wordt daarmee steeds belangrijker. Respondent ondersteunt deze ontwikkelingen met haar dienstverlening in het mobiele en vaste netwerk met verschillende diensten. Zie antwoord 15 voor verdere uitleg.

Partij 3: We zien dat verschillende gebruikers verschillende wensen hebben. Ons portfolio stelt gebruikers meer en meer in staat om ook daadwerkelijk de generieke oplossing als individuele toepassing te gebruiken. Bijvoorbeeld een aantal gebruikers dat primair gebruik maakt van een mobiele telefoon met integratie van het vaste nummer, én andere gebruikers die individueel bereikbaar zijn op UC, én een contactcenter voor hoog volume telefonie en/of specifieke functionaliteiten om de bereikbaarheid te optimaliseren.

Partij 4: Concrete ontwikkelingen op de dienst Vaste Telefonie:

In de toekomst vindt de basis van vast-mobiel integratie plaats in ons Business netwerk. Voordeel hiervan is dat de functionaliteit niet afhankelijk is van het apparaat dat de functionaliteit gebruikt. "vast nummer op mobiel" werkt op iedere mobiele telefoon. Geplande verbeteringen en uitbreidingen:

- De beschikbaarheid van een op open standaarden gebaseerde mobiele presence interface (bijv. obv XMPP) voor derde partijen, hierdoor wordt integratie met andere (cloud)platformen eenvoudiger.
- Selfcare van de vast-mobiel functionaliteit via een app op een smartphone, hierdoor kan een eindgebruiker eenvoudig bepaalde beheerszaken zelf uitvoeren.
- Een koppeling voor inkomend vast verkeer direct op mobiel, zodat een vast nummer voor zowel inkomend als voor uitgaand verkeer gebruikt kan worden op een mobiel.
- Om het nummer management te vereenvoudigen wordt het mogelijk om gebruik te maken van telefoonnummers van derde telecomoperators op het mobiele netwerk.

Een diepere integratie van vast en mobiel in Teams:

- Vast op Mobiel Status waarbij het mobiele netwerk presence integreert in onze dienst Calling in Office 365, de direct routing variant van Ons bedrijf Business. Hierdoor is altijd zichtbaar wat de status is van een mobiele aansluiting binnen de Teams client (beschikbaar, niet beschikbaar en offline).
- Integratie van Teams – native apps om nummerbeheer te managen.
- Gebruik van de DND (do not disturb) status binnen teams om actief oproepen te herrouteren.

4a

Bereikbaarheid, met name in geval van calamiteiten, is voor de rijksoverheid belangrijk. Naast dat de eigen infrastructuur van de deelnemers hier in moet voorzien, zal ook de operator een verantwoordelijkheid hebben. Welk handelingsperspectief past u toe om bereikbaarheid van rijksoverheidsinstanties te herstellen, als er in uw netwerk een dergelijke grote storing optreedt, waardoor publieke nummers niet meer te routeren zijn, of zelfs niet eens meer aangekozen kunnen worden?

Partij 1: NEC's UNIVERGE BLUE voice service omvat een reeks functies voor bedrijfscontinuïteit waarmee bedrijven kunnen blijven bellen en gebeld worden, zelfs in het geval van een lokale storing of een ernstiger noodgeval:

- > Automatische Assistent wordt gehost in het NEC UNIVERGE BLUE Netwerk en beantwoordt en routeert oproepen als een bedrijf een storing heeft.
- > Automatische herrotering naar mobiele apparaten of externe nummers als de kantoortelefoons niet beschikbaar zijn.

> Plug-and-Play verhuizing van telefoons als u snel telefoons moet verplaatsen.
> Via softphones kunnen oproepen worden ontvangen of geplaatst vanuit de UNIVERGE BLUE CONNECT Desktop-app of Mobiele app door simpelweg naar een gebied met een internetverbinding te gaan dat niet wordt beïnvloed door de storing.

Partij 2: De rijksoverheid moet te allen tijde bereikbaar blijven in geval van calamiteiten voor hulpdiensten en burgers. Als operator biedt respondent een doorschakelpakket waarmee nummers vanaf het platform doorgeschakeld kunnen worden naar andere bestemmingen. De opdrachtgever kan doorschakelingen zelf in de portal zetten en verschillende routeringen klaarzetten voor verschillende calamiteiten. Hiermee kan de opdrachtgever bereikbaar blijven in geval van calamiteiten.

Partij 3: De vaste telefoniediensten kunnen worden ingericht middels redundantie; verbindingen met verhoogde beschikbaarheid worden geleverd met twee end-to-end gescheiden routes op 1 of 2 klantlocaties en datacenters. Een beschikbaarheid tot wel 99,999% is daarmee realiseerbaar. Daarnaast levert Inschrijver voice routing, waarmee de deelnemer inkomende gesprekken in geval van een calamiteit op een andere eindbestemming kan laten afleveren. Voice routing wordt ingericht op de eerste node van het operator netwerk en is daarmee onafhankelijk van het voice routing platform. Hierdoor zijn gebruikers maximaal verzekerd van bereikbaarheid, zelfs tijdens (sporadische) storingen in het voice platform. Met verhoogde beschikbaarheid op de infrastructuur van de operator wordt maximale bereikbaarheid gecreëerd. Echter, het is van cruciaal belang dat de deelnemer ook binnen haar domein alle benodigde redundantie heeft ingebouwd om de operator redundantie effectief te laten werken.

Partij 4: Ons netwerk is voorzien van:

- Lokale redundantie
- Geografische redundantie,
- Overloop routes tussen systemen en de mogelijkheid om te herrouteren wanneer systemen 'vol' dreigen te lopen.

Hiernaast is een groot gedeelte van het netwerk gevirtualiseerd. Het is mogelijk om inkomende gesprekken aan te nemen en een bericht af te spelen om aan te geven dat er problemen zijn. Vervolgens wordt een gesprek te gerouteerd naar een ander geografisch nummer indien de omgeving van de deelnemer of onze eigen SIP trunking dienst niet naar behoren functioneert. Ook is het mogelijk een (spoed) portering van het nummer uit te laten voeren. Hiervoor is het wel noodzakelijk dat de partij waar het nummer heen geporteerd wordt enige vorm van connectiviteit paraat heeft met de deelnemer.

4b	Wat zijn voor uw netwerk de opties om bijvoorbeeld provider-overstijgende publieke nummer-routering mogelijk te maken Licht de opties svp toe.
-----------	---

Partij 1: Hiervoor lopen gesprekken tussen providers en ACM, maar concreet zijn daar nog geen acties uitgekomen.

Partij 2: We begrijpen de wens bijvoorbeeld provider- overstijgende publieke nummer-routering mogelijk te maken. Tot nu toe zijn er geen generieke afspraken gemaakt tussen de operators, om elkaars verkeer over te nemen in geval van een calamiteit waarbij het hele netwerk van de provider verstoord is. Mocht in de praktijk blijken dat de storing langer duurt, dan gaat respondent uiterste inspanning leveren om de nummers tijdelijk te porteren naar een andere operator. Ervaring vanuit het verleden is dat het in de praktijk in ons netwerk niet voorkomt. Mocht de storing zich achter het eigen platform bevinden, kunnen wij de nummers in ieder geval doorschakelen naar willekeurige nummers van alle providers.

Partij 3: PSTN nummers in Nederland zijn toegekend aan één provider. Daarin ligt een technische afhankelijkheid die hierin beperkingen oplevert. Deze situatie is voor elke operator identiek.

De basis van het netwerk is hoog beschikbaar over meerdere locaties opgebouwd. Daarnaast zijn processen en procedures ingericht om maximale beschikbaarheid van de platformen en diensten te garanderen. Doordat we een grote speler in Nederland zijn, hebben we de mogelijkheid deze diensten ook zeer betrouwbaar in te richten.

Inschrijver heeft bij de eerste node in haar netwerk calamity routing geïmplementeerd waardoor deze afhankelijkheid geminimaliseerd wordt.

Partij 4: Provider overstijgende nummerrouting (PONR) is een technologie die het mogelijk maakt om gesprekken te routeren via meerdere telecommunicatieproviders, in plaats van via één enkele provider. Dit kan worden gedaan door middel van een combinatie van software en hardware die nummerrouting analyseert en besluit welke provider het beste geschikt is voor een specifiek gesprek. Vereniging COIN voorziet in een centrale database waarin alle Nederlandse nummers staan en bij welke service provider deze nummers actief zijn. Provider overstijgende nummerrouting is iets wat niet ondersteund wordt vanuit vereniging COIN. De enige mogelijkheid die de Nederlandse Service Providers hebben is het in verwerken van een (spoed) portering. Waarbij de nummers naar een andere service provider geporteerd worden. Hiervoor is het wel noodzakelijk dat de partij waar het nummer heen geporteerd wordt enige vorm van connectiviteit paraat heeft met de deelnemer om de gesprekken af te kunnen leveren.

5	Spoofing, het zich kunnen voordoen als iemand anders, zowel op nummer als op naam komt vaker voor. De Rijksoverheid wilt dit geëlimineerd hebben. Hoe voorziet uw organisatie / netwerk / dienstverlening in waarborgen om spoofing tegen te gaan of zelfs uit te bannen? Licht uw waarborgen svp toe.
----------	---

Partij 1: Hiervoor zijn ontwikkelingen binnen de carriers/ACM/ EU gaande, maar echte stappen zijn daarin nog niet genomen. Amerika werkt met verified callers, dit wordt ook ondersteund in het UNIVERGE BLUE platform. Dit is in Nederland nog niet door de providers geïmplementeerd. Zodra deze mogelijkheid wordt geboden is dit onmiddellijk beschikbaar binnen het platform.

Partij 2: Spoofing is een erg hinderlijke en ontwrichtende die oplichters gebruiken en komt helaas voor, ook binnen Nederland. Respondent kan niet 100% waarborgen dat telefooncentrales een nummer uitsturen dat niet aan de trunk behoort die zij (de bellers) afnemen. Dit is mede afhankelijk van de security maatregelen van de andere providers. Veel klanten hebben de wens om andere nummers mee te sturen dan de lokale doorkiesnummers van de SIP trunks. Bijvoorbeeld een 0800 nummer wordt meegestuurd in plaats van het bedrijfsnummer. Respondent ontwikkelt aanvullende diensten op het gebied security. Een van deze is het analyseren, detecteren van IP-adressen gekoppeld aan de Caller-ID van de beller, zodat bijvoorbeeld een 020-nummer gekoppeld aan een Afrikaans IP-adres niet wordt doorgezet naar een medewerker van Ministerie van Economische Zaken. Verder kan afwijkend belgedrag worden gedetecteerd om vervolgens de juiste mensen binnen de organisatie op de hoogte te stellen (dashboard/Email). Een werkzame methode om spoofing tegen te gaan is door alert te zijn en spoofing te herkennen als zodanig. Een aantal voorbeelden is een neptelefoontje van uw bank, neptelefoontje met een bandje en een neptelefoontje vanuit het buitenland. Het advies is om in geen van gevallen in te gaan op deze methodieken. Dit kan door uw medewerkers voor te lichten.

Partij 3: Wij nemen via COIN deel aan de CLI spoofing taskforce en werken daarin samen met de andere operators aan een structurele oplossing om in Nederland CLI spoofing tegen te gaan. Huidige status is dat we een gemeenschappelijke blacklist aan Nederlands CLI's op onze internationale inkomende interconnect bijhouden. Op nationaal verkeer is er in Nederland geen CLI spoofing, CLI spoofed verkeer komt zo goed als altijd vanuit het buitenland. Incidentele CLI spoofing is helaas niet goed tegen te gaan zonder een gemeenschappelijk aanpak inclusief regelgeving. Wij volgen de aanbeveling vanuit de COIN CLI spoofing task force. Wij zetten in op een regelgeving waarbij we alleen NL CLI's uit het buitenland mogen weergeven die geregistreerd staan als in gebruik in het buitenland. Op basis daarvan kunnen we 99,9% op alle spoofed CLI calls inkomende op

onze internationale interconnects de CLI onderdrukken (muv CLIs van calls met roaming B-nummers).

Partij 4: Gesprekken die opgezet worden vanuit ons netwerk worden gecontroleerd op het nummer dat meegezonden wordt. Indien een nummer meegezonden wordt dat niet bij de betreffende klant hoort, wordt dit nummer vervangen door een nummer wat wel toebehoort aan deze klant. Gesprekken welke opgezet worden vanuit andere service providers en via onze interconnect binnenkomen op ons netwerk zijn niet te controleren. Het tegengaan van nummer spoofing en robocalls is een veelbesproken onderwerp tussen de verschillende nationale providers en ACM. Een mogelijke oplossing is het STIR/SHAKEN framework (Secure Telephony Identity Revisited / Signature-based Handling of Asserted information using tokens). Hierbij wordt het meegezonden nummer gecontroleerd aan de hand van authenticatie en certificaten. Een dergelijke implementatie is echter niet gemakkelijk en dient bij zowel de initiërende partij (nationaal en internationaal) als bij de ontvangende partij gerealiseerd te worden. Een oplossing voor spoofing kan alleen worden gerealiseerd in de samenwerking tussen de verschillende providers, eenzijdig is een volledig afgedekte oplossing niet haalbaar omdat de afstemming tussen providers ontbreekt. Internationaal is het nog complexer om deze afspraken vast te leggen.

6	Social engineering en hacking zijn hot topics. De Rijksoverheid wilt dit geëlimineerd hebben. Hoe voorziet uw organisatie / netwerk / dienstverlening in waarborgen om deze activiteiten tegen te gaan of zelfs uit te bannen? Licht uw waarborgen svp toe.
----------	--

Partij 1: U kunt erop vertrouwen dat uw privé- en bedrijfsgegevens veilig zijn bij NEC. Ons systeem maakt gebruik van de modernste technologieën die zijn ontworpen om voortdurend te controleren op en te verdedigen tegen kwaadwillende indringers. Het NEC UNIVERGE BLUE-beveiligingsplatform omvat vijf primaire beveiligingspijlers die zich voortdurend ontwikkelen en aanpassen om op elke mogelijke dreiging te reageren en effecten te beperken. Deze vijf pijlers worden regelmatig onderzocht en herzien door het beveiligingsteam van NEC om ervoor te zorgen dat onze klanten een superveilige communicatie- en samenwerkingsservaring hebben die kan worden vertrouwd om hen en hun bedrijven te beschermen. Het Voice Cloud-netwerk van NEC levert 99,999% (vijf negens) uptime voor onze spraakdiensten. We ondersteunen onze uptime-garantie van 99,999% met een financieel gedekte Service Level Agreement. Dit betrouwbaarheidsniveau - dat neerkomt op minder dan 26 seconden ongeplande downtime per maand - is mogelijk omdat onze architecten en ingenieurs hun diepgaande expertise hebben toegepast op zeven belangrijke technologische componenten:

Partij 2: Social engineering en hacking zijn net als spoofing in potentie ondermijnende activiteiten. Respondent heeft diensten ontwikkeld die er op gericht zijn om deze activiteiten tot een minimum te beperken. Digitale veiligheid is een belangrijk onderdeel geworden van de bedrijfsvoering binnen de rijksoverheid. Toch zijn niet alle medewerkers zich even goed bewust van digitale risico's en hoe hun eigen gedrag deze beïnvloeden. Om medewerkers dit bewustzijn bij te brengen en hen onderdeel te maken van uw securitybeleid, bieden wij het Security Awareness Programma. Het Security Awareness Program helpt organisaties bij het opzetten en implementeren van een veiligheidsprogramma dat medewerkers onderdeel maakt van de securitystrategie. Het maatwerkprogramma is geschikt voor medewerkers van alle niveaus en creëert bewustzijn over digitale veiligheid en gedrag. De voordelen van dit programma zijn:

- Versterkt uw verdediging doordat uw medewerkers volwaardig onderdeel worden van de securitystrategie;
- Verlaagt risico's en kosten want incidenten worden gemitigeerd en voorkomen door bewustzijn en gedrag van medewerkers;
- Bewezen veilig en effectief, is ISO 27001 compliant en ontwikkeld met gerenommeerde partners.

Voordat Respondent diensten introduceert worden PEN-testen uitgevoerd, waarmee de security verbeterd. Dat is één maatregel om te voorkomen dat hackers succes hebben. Daarnaast voert ons bedrijf de managed service Next Generation SIP Security (NGSS) in het portfolio. Deze dienst is specifiek ontwikkeld met als uitgangspunt de beveiliging van het Session Initiation Protocol (SIP) met in achtname van geldende wet- en regelgeving. NGSS biedt VoIP en UC perimeter beveiliging gelijk aan een SBC én meer. Waar een SBC traditioneel wordt ingezet om controle te krijgen over de VoIP-signalering en over de datastromen die nodig zijn voor het opzetten van een telefoongesprek, het voeren van een telefoongesprek en het afbreken van een telefoongesprek, gaat NGSS veel verder. NGSS is een effectieve UC/VoIP beveiligingsoplossing die, naast maximale beveiliging, voldoet aan compliance en auditvereisten in real-time communicatie.

Partij 3: Inschrijver is ISO27001 gecertificeerd en laat jaarlijkse penetratietesten uitvoeren. Er is een Security team met alle benodigde disciplines ingericht dat verantwoordelijk is voor de dagelijkse beveiliging van de diensten in de breedste zin van het woord. Er worden hackatons georganiseerd en er worden regelmatig phishing campagnes georganiseerd om de security awareness binnen de organisatie te verhogen. Er is digitale en fysieke beveiliging op de kantoor-en datacenterlocaties en op alle locaties vindt toegangscontrole plaats.

Vanuit technisch perspectief zijn de SIP diensten van inschrijver volledig gescheiden van het publieke internet, op de interfaces is slechts SIP verkeer toegestaan en geen andere protocollen.

Partij 4: Social engineering is het gebruik van psychologische manipulatie om mensen te misleiden tot het prijsgeven van gevoelige informatie of het uitvoeren van acties die niet in hun beste belang zijn. De essentie hierbij is dat de mens de zwakste schakel is in elk beveiligingssysteem. Social hacking, ook wel bekend als 'human hacking' is een vorm van social engineering waarbij de aanvaller gebruik maakt van menselijke interactie en emoties om informatie of toegang te verkrijgen. Er is een onderscheid tussen fysieke en digitale Social Engineering.

Voorbeelden van fysieke engineering zijn:

- Tailgating: Dit is het volgen van iemand door een beveiligde deur zonder daadwerkelijk te worden uitgenodigd of te laten zien wie je bent.
- Distractie: Dit is het afleiden van een persoon terwijl iemand anders de gelegenheid krijgt om informatie of toegang te verkrijgen.
- Shoulder surfing: Dit is het observeren van iemand die gevoelige informatie invoert, zoals een wachtwoord of pincode, over iemands schouder.
- Spear phishing: Dit is het gerichte benaderen van een specifieke persoon of organisatie met een e-mail of telefoontje, waarbij de aanvaller zich voordoeft als iemand van vertrouwen om informatie of toegang te verkrijgen.
- Dumpster diving: Dit is het doorzoeken van afvalbakken op zoek naar gevoelige informatie die kan worden gebruikt voor social engineering.

Digitale social engineering is het gebruik van digitale middelen, zoals e-mails, websites, sociale media en telefoontjes, om informatie of toegang te verkrijgen. Voorbeelden van digitale social engineering zijn:

- Phishing: Dit is het versturen van e-mails of berichten die eruit zien als ze afkomstig zijn van een betrouwbare bron, zoals een bank of een bedrijf, om gevoelige informatie te verkrijgen.
- Vishing: Dit is het gebruik van telefoontjes om gevoelige informatie te verkrijgen, bijvoorbeeld door zich voordoen als een bedrijf of organisatie.
- Pretexting: Dit is het verzinnen van een smoes om gevoelige informatie te verkrijgen, zoals door zich voor te doen als een werknemer van een bedrijf of overheidsfunctionaris.
- Baiting: Dit is het aanbieden van iets waardevols, zoals een gratis download of een prijs, om gevoelige informatie te verkrijgen.
- Quid pro quo: Dit is het vragen om een gunst in ruil voor informatie of toegang.
- Spear phishing: Dit is gericht phishing gericht op specifieke personen of organisaties.
- Ransomware: Dit is malware die bestanden versleutelt en eist om een losgeld te betalen voor de ontsluiting.
- Malware: Dit is software die onbedoelde gevolgen kan hebben voor een computer of netwerk, zoals het verzamelen van gevoelige informatie of het sturen van spam.

Bij onze Business dienst is er veel aandacht voor Social Engineering, alle medewerkers moeten jaarlijks een training volgen op het gebied van security en social engineering. Ook worden er op gezette tijden penetration tests uitgevoerd. Ook phishing awareness campagnes worden regelmatig uitgevoerd. Deze programma's en activiteiten om het bewustzijn van onze medewerkers op dit gebied te vergroten voeren wij ook bij onze klanten uit. Naast deze activiteiten voldoen we ook aan de geldende wet en regelgeving vanuit de overheid voor operators en hebben we vanuit onze moederbedrijven strikte governance en auditing ingeregeld. Hiernaast is onze dienst Business ISO27001 gecertificeerd.

7a	Geef svp een toelichting op de ontwikkeling van SIP OTT (zonder de noodzaak van CPE) in relatie tot uw eigen huidige dienstverlening?
-----------	--

Partij 1: Als er een wens is om SIP OTT te gebruiken dan kan dat d.m.v. bring your own trunk en een session border controller worden aangesloten op het platform.

Partij 2: De bestaande dienst van respondent is gebaseerd op een SIP trunk over internet. Zij levert deze dienst vanuit geografisch gespreide redundante datacenters inclusief internetconnectiviteit. Hiervoor is geen CPE vereist. Deze dienst kan op basis van het TLS protocol communiceren met bijvoorbeeld de tenant van MS Teams. Het is ook mogelijk om met een SBC (van klanten) te communiceren, mits deze via internet bereikbaar is via een IP-adres. Vast-mobiel integratie is momenteel vanuit deze dienst beschikbaar voor de Cisco Cloud oplossing. Ontwikkelingen zitten vooral in de vast-mobiel integratie met cloud communication oplossingen zoals MS Teams en Genesys.

Partij 3: De SIP diensten van Inschrijver zijn volledig gescheiden van het publieke internet, op de interfaces is slechts SIP verkeer toegestaan en geen andere protocollen. Bij routing van diensten over publiek internet is het niet mogelijk kwaliteit te garanderen (Internet is best effort dienstverlening). OTT SIP diensten zijn daarmee uitgesloten van garanties. OTT SIP voor individuele gebruikers biedt vaak voldoende zekerheid voor een individuele gebruiker. Deze worden derhalve vaker toegepast achter de PBX, bijv. in UC of Teams toepassingen.

Partij 4: SIP OTT staat voor "Session Initiation Protocol over Over-the-Top." OTT verwijst naar de levering van diensten, zoals spraak- en videocommunicatie, via internet, zonder tussenkomst van traditionele telecommunicatieproviders. SIP OTT is het gebruik van het SIP-protocol om communicatiesessies via internet te initiëren en te beheren, in plaats van via een traditioneel telefoonnetwerk. Er zijn een aantal risico's als het gaat om het gebruik van SIP OTT:

- Beveiligingsrisico's: Omdat SIP OTT-communicatie via internet verloopt, zijn er meer risico's op hackers die toegang proberen te krijgen tot privégegevens, zoals wachtwoorden en creditcardgegevens.
- Kwaliteit van de verbinding: Omdat SIP OTT afhankelijk is van een goede internetverbinding, kan de kwaliteit van de verbinding variëren, vooral in gebieden met een slechte internetdekking.
- Interoperabiliteit: Sommige SIP OTT-diensten zijn alleen compatibel met bepaalde apparaten of besturingssystemen, wat problemen kan veroorzaken bij het gebruik van meerdere apparaten of verschillende besturingssystemen.
- Toezichhoudend: Omdat SIP OTT geleverd kan worden zonder de traditionele en gereguleerde telecommunicatieproviders, is er geen toezicht op de kwaliteit en beveiliging van de dienst.
- Afhankelijkheid van internet: SIP OTT diensten zijn afhankelijk van internet verbinding, dus als er een internet onderbreking is werkt de dienst niet.

Voordelen van SIP OTT

- Lagere kosten: SIP OTT-diensten zijn vaak goedkoper dan traditionele telefoniediensten, vooral voor internationale gesprekken.
- Flexibiliteit: SIP OTT-diensten kunnen worden gebruikt op verschillende apparaten, zoals smartphones, tablets en computers, waardoor ze gemakkelijk kunnen worden meegenomen en gebruikt op verschillende locaties.

- Verhoogde productiviteit: SIP OTT-diensten bieden vaak geavanceerde functies, zoals videoconferencing en instant messaging, die de communicatie tussen medewerkers kunnen verbeteren en hun productiviteit verhogen.
- Scalability: SIP OTT-diensten zijn vaak eenvoudig te schalen, zodat ze kunnen worden aangepast aan de groeiende behoeften van een organisatie
- Mobiele communicatie: Omdat SIP OTT via internet verloopt, is het gemakkelijk te gebruiken op mobiele apparaten, waardoor medewerkers gemakkelijk kunnen communiceren terwijl ze onderweg zijn.
- VoIP technologie: SIP OTT is gebaseerd op VoIP technologie, dus het biedt veel van dezelfde voordelen, zoals de mogelijkheid om te integreren met andere zakelijke applicaties zoals CRM of helpdesk software.

Ons bedrijf onderzoekt momenteel hoe wij SIP OTT diensten kunnen aanbieden die voordelen bieden voor onze klanten, maar tegelijkertijd voldoende bescherming bieden tegen de risico's van OTT diensten.

7b Kunt u de onder vraag 7a bedoelde vorm van dienstverlening SIP OTT nu of in de komende 12 maanden aanbieden? Zo nee, op welke termijn bent u daartoe wel bereid en in staat?

Partij 1: Het platform is al klaar d.m.v. bring your own trunk om een sip ott oplossing te connecteren.

Partij 2: De onder 7a eerste alinea beschreven dienstverlening is nu al beschikbaar. Respondent heeft de vast-mobiel integratie met cloud communication oplossing MS Teams en Genesys binnen een half jaar operationeel.

Partij 3: Zie bovenstaand antwoord.

Partij 4: Ons bedrijf heeft op dit moment verschillende OTT oplossingen en voor specifieke doelgroepen. Wij onderzoeken momenteel hoe wij SIP OTT diensten kunnen aanbieden die voordelen bieden voor onze grootzakelijke klanten, maar tegelijkertijd voldoende bescherming biedt tegen de risico's van OTT diensten. Het is onze verwachting dat wij in de komende 12 tot 24 maanden een duidelijke oplossingsrichting hiervoor hebben, of deze diensten dan ook direct leverbaar zijn voor de grootzakelijke markt is op voorhand nog niet te zeggen. Dit is afhankelijk van de verhouding tussen investeringskosten, verwachte return on investment en vraag vanuit de markt.

7c Geef svp een toelichting, hoe door uw organisatie bij CPE- aansluitingen wordt omgegaan met vereisten van security en versleuteling van de verbinding.

Partij 1: Zie onze beantwoording bij vraag 6 waar dit onderdeel van uit maakt.

Partij 2: Veiligheid zit ingebouwd in het DNA van al onze diensten. De diensten en geleverde hardware voldoen aan alle standaarden voor beveiliging. Zoals eerder aangegeven is het uitvoeren van PEN-testen onderdeel van de dienstverlening, waarmee de security verbetert. Daarnaast worden ook onze Security Policy richtlijnen toegepast. Deze combinatie zorgt ervoor dat de dienstverlening voldoet de zwaarste security richtlijnen in de ICT sector.

Partij 3: De routing van verkeer in ons netwerk is volledig gescheiden van publiek internet. Door het gesloten karakter van ons netwerk is inbreuk hierop niet mogelijk, en is encryptie daarop in principe onnodig. Inschrijver voorziet encryptie op netwerken als add-on, maar ziet de toepassing hiervan als standaard oplossing binnen spraak niet als marktzens. Routing van PSTN verkeer over internet (waar) encryptie wel gewenst en noodzakelijk is, wordt door inschrijver als ongewenst gezien.

Partij 4: Zoals eerder aangegeven is onze business ISO27001 gecertificeerd. In ons beveiligingsplan liggen de afspraken en maatregelen vast die wij op ons netwerk en onze netwerkcomponenten van toepassing zijn. Hiernaast maken wij voor onze SIP diensten gebruik van een IP-VPN (Internet Protocol Virtual Private Network). Dit specifieke netwerk is alleen voor de gebruiker en wordt niet gedeeld met andere VPN gebruikers.

Dit biedt grotere veiligheid en controle over de netwerktoegang, evenals de mogelijkheid om het IP-adres te gebruiken voor specifieke toepassingen of diensten. Het is mogelijk om versleuteling toe te passen op SIP verbindingen. Voorbeelden hiervan zijn:

- SRTP (Secure Real-time Transport Protocol): SRTP is een protocol dat is ontworpen om realtime audio- en videostreams te versleutelen. Het kan worden gebruikt om SIP-verbindingen te beveiligen tegen af luistering en manipulatie.
- TLS (Transport Layer Security): TLS is een protocol dat wordt gebruikt om een veilige verbinding te maken tussen twee systemen, zoals een SIP-telefoon en een SIP-server.
- SIPS (SIP Secure): SIPS is een protocol dat is gebaseerd op SIP, maar met extra beveiligingsfuncties, zoals certificaat gebaseerde authenticatie en versleuteling.
- ZRTP (Zimmermann Real-time Transport Protocol): ZRTP is een protocol dat is ontworpen voor real-time versleuteling van audio- en videostreams.
- Het is belangrijk om te weten dat de beveiliging van SIP-verbindingen afhankelijk is van de implementatie ervan, dus het is belangrijk om te werken met een betrouwbare provider die ervaring heeft met het beveiligen van SIP-verbindingen. Deze opties zijn op dit moment geen onderdeel van onze standaarddienstverlening.

8 Self-service vanuit een portal waar de afgenomen diensten en onderliggende functionaliteiten door de opdrachtgever zelf te beheren en aan te passen zijn, is belangrijk. Zijn de onderstaande functionaliteiten real-time in uw netwerk/dienstverlening voor opdrachtgever beschikbaar? Geef per item svp een beknopte toelichting.

- 1. Trunk nummer management en nummer hertoewijzing tussen trunks.**
- 2. Handmatig doorschakelen van nummers naar alternatieve nummers.**
- 3. Automatisch doorschakelen van nummers naar alternatieve nummers ingeval een trunk onbeschikbaar is.**
- 4. Monitoren status van de SIP Trunk en aanpalende verbindingen.**
- 5. Mogelijkheid om monitoring data op basis van bijvoorbeeld SNMP, Syslog of een beschreven API te exposen naar interne beheer tooling van opdrachtgever.**
- 6. Mogelijkheid om gesprekkosten door te belasten op basis van door opdrachtgever zelf te definiëren, eventueel trunk overstijgende nummer groepen en afdelingen.**
- 7. Mogelijkheid voor opdrachtgever om zelf SIP debug traces te doen.**
- 8. Zoekfunctie op telefoonnummer of deel van een telefoonnummer.**

Partij 1:

- 1) N.v.t.
- 2) Ja kan via portal
- 3) Bij Trunk als IaaS niet nodig want trunk altijd beschikbaar, bij Bring your own Trunk instelbaar in SBC
- 4) Bij Trunk als IaaS niet nodig want trunk altijd beschikbaar, bij Bring your own Trunk zichtbaar in SBC
- 5) Platform kent diverse api's om data te verkrijgen of onderdelen aan te sturen.
<https://developer.univerge.blue/api/spec/analytics/index.html>
- 6) In overleg moeten we kijken wat de mogelijkheden zijn
- 7) Alleen in geval Bring your own Trunk via de SBC
- 8) Ja is mogelijk.

Partij 2: Vanzelfsprekend biedt respondent klanten een self-service portal aan van waaruit key-users en beheerders vanuit de klantorganisatie zonder tussenkomst van onze medewerkers functionaliteiten kunnen activeren of deactiveren en rapportages kunnen opvragen. Er zijn veel basisfunctionaliteiten beschikbaar. De ontwikkeling van bestaande of nieuwe functionaliteiten in het portal is een gegeven. In het bijzonder vraagt u de specifieke mogelijkheden naar een aantal functionaliteiten van het portal:

1. trunk nummer management en nummer hertoewijzing tussen trunks zijn functionaliteiten die niet via de portal beschikbaar zijn. Uiteraard zijn deze wel als change aan te vragen via de servicemanager;
2. het handmatig doorschakelen van nummers naar alternatieve nummers is mogelijk

in de portal;

3. het automatisch doorschakelen van nummers naar alternatieve nummers als een trunk onbeschikbaar is, is mogelijk in de portal;

4. Respondent monitort de status van de SIP trunk en aanpalende verbindingen maar dit is nog niet voor de opdrachtgever beschikbaar in een portal; graag vernemen we wat uw specifieke wensen zijn m.b.t. deze functionaliteit;

5. Respondent zal de monitoring data afkomstig van de dienst in de toekomst beschikbaar maken in een dashboard in de portal; voor de VPN routers is die nu al beschikbaar (SNMP);

6. het is mogelijk om trunks of nummers aan verschillende debiteuren toe te wijzen; op debiteuren niveau wordt er gefactureerd; een debiteur in dit kader is een onderdeel binnen de opdrachtgever met een eigen debiteurnummer;

7. de mogelijkheid voor opdrachtgever om zelf SIP debug traces te doen kunnen wij op verzoek mogelijk maken;

8. de functionaliteit zoekfunctie op telefoonnummer of deel van een telefoonnummer wordt momenteel gepresenteerd als een lijst in de portal; in de toekomst wordt hier een zoekfunctie op gemaakt.

Partij 3:

1. Trunk nummer management en nummer hertoewijzing tussen trunks. Middels een wijzigingsverzoek via de portal kan dit worden aangevraagd.

2. Handmatig doorschakelen van nummers naar alternatieve nummers.

Inschrijver biedt Voice routing, waarmee de deelnemer inkomende gesprekken op een andere eindbestemming kan afleveren. Deze functionaliteit is door de deelnemer te (de)activeren via een webportal. Voice Routing biedt controle over herrouteringen voor de belangrijkste telefoonnummers en/of nummerblokken. De klant bepaalt zelf wanneer en voor hoelang hij deze herrouteringen activeert. Hiermee blijft de klant toch bereikbaar bij calamiteiten, gepland onderhoud of voor een langdurige doorschakeling naar nieuw geïntroduceerde telefoonnummers (na bijvoorbeeld een verhuizing).

3. Automatisch doorschakelen van nummers naar alternatieve nummers ingeval een trunk onbeschikbaar is. Middels verhoogde beschikbaarheid worden SIP trunks redundant geconfigureerd op 1 of 2 klantlocaties en datacenters. Door de active/active configuratie van de beide SIP trunks worden nummerblokken op beide SIP trunks afgeleverd. Daarnaast is het voor de deelnemer mogelijk om inkomende gesprekken op een andere eindbestemming af te leveren (zie hierboven).

4. Monitoren status van de SIP Trunk en aanpalende verbindingen.

Het netwerk van de Inschrijver, inclusief de backbone apparatuur, wordt 24 uur per dag en 7 dagen per week bewaakt en onderhouden door het Network Operations Center (NOC). Het NOC beschikt over geavanceerde hulpmiddelen waarmee op netwerkproblemen kan worden geanticipeerd. Het NOC bewaakt de continuïteit van de dienstverlening en onderneemt waar nodig acties om kwaliteitsvermindering van de dienst te voorkomen.

5. Mogelijkheid om monitoring data op basis van bijvoorbeeld SNMP, Syslog of een beschreven API te exposen naar interne beheer tooling van opdrachtgever.

Inschrijver staat dit niet toe omdat de CPE zich in het domein van de inschrijver (operator) bevindt.

6. Mogelijkheid om gesprekkosten door te belasten op basis van door opdrachtgever zelf te definiëren, eventueel trunk overstijgende nummer groepen en afdelingen. Facturatie vindt plaats per SIP dienst. Opdrachtgever zou pro rata van het gebruik van de diensten kunnen doorbelasten aan de hand van de door de Inschrijver verstrekte CDR's.

7. Mogelijkheid voor opdrachtgever om zelf SIP debug traces te doen.

Dit is niet mogelijk. Middels het incidentmanagementproces biedt Inschrijver ondersteuning bij het onderzoeken.

8. Zoekfunctie op telefoonnummer of deel van een telefoonnummer.
In de webportal is het opzoeken van telefoonnummer mogelijk.

Partij 4:

1. Deze handeling is geen onderdeel van de selfservice mogelijkheden. Wijzigingen kunnen via de portal worden aangevraagd en worden vervolgens door de supportafdelingen uitgevoerd.

2. Dit is niet mogelijk via onze portal, doorschakelen is een functionaliteit die wordt ingesteld in de PABX of telefooncentrale. Bij een SaaS oplossing gaat dit via de gebruikersomgeving.

3. Emergency Routing Service is een onderdeel van SIP oplossing. Via de portal kan dit worden ingesteld.

4. De fysieke verbindingen zijn te monitoren via de portal, specifieke status van de SIP trunk niet aangezien dit een 'service' is die op de verbinding wordt geplaatst.

5. SNMP access op apparatuur is geen onderdeel van onze standaarddienstverlening. Er zijn ook geen API's beschikbaar om onze tooling te koppelen aan de tooling van opdrachtgever zijn niet aanwezig.

6. Dit is mogelijk via onze portal op basis van de extra module Expense Management.

7. Dit is mogelijk van de telefooncentrale van de opdrachtgever.

8. Dit is mogelijk via de eerdergenoemde module Expense Management

9	Ondersteuning voor IPv6 wordt steeds belangrijker. Kunt u End2End routing voor IPv6 zowel in het interne netwerk van deelnemers als naar ITSP leveren? Zo ja, geef svp een korte beschrijving van deze mogelijkheid.
----------	---

Partij 1: Nee.

Partij 2: Respondent herkent dat het belang van de ondersteuning voor IPv6 toeneemt. Momenteel wordt IPv6 routing End2End nog niet ondersteund. Binnen de zakelijke dienstverlening zijn nog voldoende IP-ranges beschikbaar, waardoor de noodzaak van IPv6 er nog niet is. Zodra de krapte in IPv4 zich voordoet, zal respondent deze zienswijze heroverwegen.

Partij 3: Inschrijver ondersteunt IPv6 op internet verbindingen. Op dit moment zien we nog slechts zeer beperkt gebruik van IPv6 op SIP. Inschrijver zal dit ondersteunen op onze toekomstige proposities in lijn met de ontwikkelingen in de markt.

Partij 4: End-to-end routing met IPv6 voor SIP betekent dat verkeer tussen SIP-clients direct wordt gerouteerd zonder tussenkomst van een gateway of een ander tussenstation. Dit betekent dat het verkeer tussen SIP-clients een directe verbinding heeft en dat de kwaliteit van de verbinding wordt verbeterd. Het gebruik van IPv6 in combinatie met SIP kan ook helpen bij het oplossen van problemen met NAT (Network Address Translation) die vaak voorkomen bij het gebruik van IPv4. Op dit moment hebben wij nog geen IPv6 ingericht voor ons SIP netwerk. Het core netwerk van ons bedrijf is inmiddels wel volledig geschikt gemaakt voor IPv6. Dit houdt in dat het er geen technische beperkingen zijn om dit in te richten. Echter tot op heden zijn er op dit gebied nog weinig tot geen behoeften geuit van onze klanten.

10a	Beschrijf svp welke kwaliteitsniveaus u onderscheidt in uw standaard dienstverlening.
	Partij 1: Er wordt altijd de hoogste kwaliteit en beschikbaarheid van de dienst gegarandeerd, daar tussen zitten geen verschillende kwaliteitsniveaus met verschillende prijsings. Partij 2: Respondent biedt één kwaliteitsniveau voor haar klanten. De kwaliteit van het voiceverkeer wordt bepaald door de bandbreedte, packet loss, jitter en delay. Er wordt geen compressie toegepast binnen de PSTN omgeving (G711 codec), waardoor een hoge audiokwaliteit (MOS boven 4.03) wordt gerealiseerd. We hebben ruime bandbreedte tussen PSTN omgeving en de omgeving van klanten. Deze omgeving wordt continu gemonitord door ons Security Operations Center (SOC). Vanuit dit SOC beveiligen en bewaken onze securityspecialisten onze ICT-infrastructuur en die van haar klanten 24 uur per dag, 7 dagen per week, 365 dagen per jaar. Partij 3: Inschrijver hanteert voor haar standaard dienstverlening kwaliteitsniveaus die worden weergegeven in verschillende Service Level Parameters. Hierbij wordt een onderscheid gemaakt in de niveaus Office SLA, Retail SLA en Premium SLA. Deze zijn marktconform. Voor VoIP aansluitingen biedt Inschrijver standaard het hoogste kwaliteitsniveau van Premium SLA aan. De niveaus worden in een beschikbaar gestelde tabel weergegeven. Inschrijver kent aan elk incident een prioriteit toe volgens een in de markt gangbaar model. Inschrijver voert regelmatig gepland onderhoud op faciliteiten of onderdelen van de dienstverlening om zo de kwaliteit en de continuïteit van onze diensten te blijven waarborgen. Gepland of preventief onderhoud bestaat uit werkzaamheden aan het bestaande netwerk of aan gerelateerde diensten van Inschrijver of toeleveranciers. De werkzaamheden worden zoveel mogelijk uitgevoerd binnen het onderhoudswindow tussen 04.00 en 07.00 uur tijdens werkdagen. Geplande werkzaamheden worden 10 werkdagen van tevoren aangemeld onder vermelding van tijd, dienst en locatie waar de werkzaamheden betrekking op hebben. Partij 4: In de basis zijn kwaliteitsniveaus aanwezig waarop ondersteuning geleverd wordt op basis van kantoor tijden, winkeltijden en 24/7. Onze standaarddienst wordt geleverd op basis van eigen infrastructuur die via een IPVPN met bijbehorende garanties met betrekking tot beschikbaarheid en gesprekkwaliteit. Hiernaast wordt ons netwerk continu actief gemonitord. Er worden proactief herstelacties geïnitieerd indien er zich calamiteiten in de dienstverlening voordoen. In onze portal worden zijn deze acties te volgen (proactive ticketing). OTT diensten maken gebruik van het openbare internet en bieden niet de betrouwbaarheid en beschikbaarheid van een dienst over dedicated infrastructuur.
10b	Welke beschikbaarheidspercentages kunnen door uw netwerk 7 x 24 x 365 gegarandeerd worden?
	Partij 1: 99,999 Uptime en ondersteuning Onze support services bieden: > 24x7x365 technische ondersteuning. Wij staan altijd voor u klaar. > Ondersteuning op drie niveaus en direct contact met ontwikkelingsteams en engineeringteams. > Geografisch verspreid team voor redundantie en 24x7 ondersteuning. > Omnichannel communicatie; Voice, email, SMS en chat. Partij 2: Respondent biedt beschikbaarheidspercentages op connectiviteit via internet en VPN. Internet. Connectiviteit via twee soorten Internet verbinding: Standaard Internet (overbooked/geen gegarandeerde bandbreedte) en premium internet waarbij de gewenste bandbreedte gegarandeerd is. Bij premium internet wordt er ook hogere beschikbaarheid geboden door redundante apparatuur (glasswitches/routers en separate glasverbindingen) naar verschillende lokale POP's (Point-Of-Presence/wijkcentrales).

Om prioritering en extra rapportagemogelijkheden te bieden van internetverkeer kan opdrachtgever gebruik maken van de SD-WAN diensten. VPN:

- Een gesloten netwerk met gegarandeerde bandbreedte voor klantlocaties;
- Beschikbaarheidsopties voor redundantie redundant Apparatuur
- Connectiviteit naar buitenwereld/internet via Central Firewall (managed dienstverlening inclusief flexibele bandbreedte)

De beschikbaarheid is afhankelijk van de drager (koper/glas), redundantie van de hardware (routers/switches) en single/dual PoP's, voor het netwerk (Premium Internet/VPN). Voor het netwerk kunnen we een beschikbaarheid realiseren van 99,98%, en voor het platform met geo-redundantie 99,99%.

Partij 3: Voor SIP diensten is de standaard beschikbaarheid 99,9%. Middels redundante verbindingen levert Inschrijver hogere beschikbaarheden. De vaste telefoniediensten kunnen eveneens worden ingericht met redundantie; verbindingen met verhoogde beschikbaarheid worden geleverd met twee end-to-end gescheiden routes op 1 of 2 klantlocaties en datacenters. Een beschikbaarheid tot wel 99,999% is daarmee realiseerbaar.

Partij 4: De beschikbaarheidspercentages worden bepaald door de zwakste schakel in de keten. Voor vaste telefoniediensten is dit de onderliggende infrastructuur.

- Beschikbaarheid van het SIP platform inclusief hosted voice diensten $\geq 99,9\%$
- Beschikbaarheid op basis van xDSL $\geq 99,6\%$
- Beschikbaarheid op basis van glasvezel $\geq 99,9\%$
- Beschikbaarheid op basis van COAX $\geq 99,6\%$

10c	Geef svp een beschrijving van de wijze waarop u de gesprekskwaliteit over uw netwerk meet. Welke parameters gebruikt u hierbij?
------------	--

Partij 1: Onze Voice Cloud wordt proactief gemonitord om de hoogste gesprekskwaliteit voor klanten mogelijk te maken. Terwijl oproepen door de Voice Cloud en de verschillende netwerkcomponenten (PBX'en, SBC's en netwerkroueters) stromen, verzamelt elk onderdeel statistieken. De statistieken worden toegevoegd aan call-detail-records, die vervolgens worden toegevoegd aan een interne database. Elke minuut doorzoeken interne systemen de database op zoek naar problemen met betrekking tot verbindingsverlies, latentie (pakketten die te lang duren om aan te komen), jitter (inconsistentie in pakkettiming) en pakketverlies (weggevalen pakketten als gevolg van congestie) op een per trunk basis. Door constant elke oproep nauwgezet te bewaken, kan het systeem automatisch of handmatig ingrijpen en QoS-problemen oplossen zonder enige tussenkomst van de klant. Door onze volledige Voice Cloud voortdurend te bewaken, worden bovendien realtime analyse van regionale en carrier-problemen uitgevoerd, waardoor proactieve evaluatie van de prestaties van de carrier mogelijk is en carriers worden geëlimineerd die spraakoproepen van hoge kwaliteit verhinderen.

Partij 2: Ons SOC is het grootste security operations center in Nederland. Vanuit daar beveiligen en bewaken onze securityspecialisten onze ICT-infrastructuur en haar klanten 24 uur per dag, 7 dagen per week, 365 dagen per jaar. Het SOC wordt gealarmeerd bij substantieel verlies aan audiokwaliteit en neemt dan actie. We zullen in de toekomst deze signalering ook beschikbaar maken voor opdrachtgever in de portal. De Mean Opinion Score (MOS)-waarde is hiervoor de belangrijkste parameter.

Partij 3: Inschrijver biedt call performance monitoring c.q. rapportage. Hierin worden onder meer call statistieken en capaciteit weergegeven.

Partij 4: Ons bedrijf Business meet de gesprekskwaliteit over het netwerk op basis van de MOS waarde (Mean Opinion Score). MOS is een maatstaf of statistiek die wordt gebruikt om de VoIP-oproepkwaliteit of audiokwaliteit te meten. De MOS waarde wordt berekend aan de hand van een aantal indicatoren:

- Reproduction Delay
- Packetization Delay
- Jitterbuffer

- Packet loss

- Packets per second

De MOS waarde wordt door ons berekend op basis van proactieve meting op het netwerk. De waarden worden berekend op basis van het totale netwerk. Er worden geen klantspecifieke MOS waarden berekend. Hiernaast meten wij ook algemene callscenarios worden gemeten met verschillende providers. De resultaten hiervan worden meegenomen in de algemene MOS waarde.

11a	Geef svp een beschrijving van de functionaliteit die uw dienstverlening biedt, waar het gaat om mobiel/smartphone gebruik in de context van bereikbaarheid onder een 06 of "vast" nummer? Denk hierbij aan Data only of native mobiel.
------------	---

Partij 1: Mobiele apparaten zoals een Tablet en smartphone hebben een mobiel integratie op native dealer. Vanuit de native dealer kan je dus met gewenst nummer uitbellen. De applicatie UB wordt dan aangeroepen. Onze visie is dat het 06 nummer expliciet wordt gebruikt voor privé verkeer en het vaste 088-en groep/hoofdnummer zakelijk. Je krijgt op je mobiele apparaten een glazenwand en kunt vooraf programmeren op contact niveau met welk gewenste nummer je wilt uitbellen.

Partij 2: De integratie van vaste en mobiele telefonie combineert de flexibiliteit van mobiel bellen met smartphones van uw medewerkers met het gemak van het nummerplan van vaste telefonie en de achterliggende telefoniecentrale of het contactcenter platform. Dit betekent onder meer dat uw mobiele telefoon verkorte interne nummers kan bellen die normaliter niet te gebruiken zijn vanuit het publieke telefonienetwerk. Daarnaast is uw mobiele telefoon ook bereikbaar op uw eigen verkorte nummer. Voor de integratie van vast bellen en mobiele telefonie is het noodzakelijk dat beide diensten van één partij worden afgenomen. De exacte werking van vast-mobiele integratiefuncties is afhankelijk van de mogelijkheden die uw telefooncentrale ondersteunt. In onderstaande beschrijving lichten we de belangrijkste functionaliteiten verder toe.

Bellen: Het mobiele netwerk zorgt ervoor dat mobiele nummers worden gekoppeld aan een vast nummer. Dit kan een lang vast en extern bereikbaar nummer zijn en een intern verkort vast nummer. Medewerkers van opdrachtgever kunnen ervoor kiezen om alleen een lang of alleen een kort intern nummer te koppelen aan het mobiele nummer. De belkosten worden bepaald door het toestel waarmee gebeld wordt en het abonnement dat daaraan gekoppeld is.

Gebeld worden: Zowel het vaste als mobiele toestel van een medewerker gaan gelijktijdig rinkelen bij een oproep op het verkorte of lange vaste nummer. Als de medewerker direct op zijn/haar mobiele nummer wordt gebeld, gaat ook de vaste telefoon rinkelen. Nummerweergave Medewerkers kunnen zelf kiezen met welke uitgaande identiteit wordt gebeld. Met behulp van de MijnGesprek app wisselen medewerkers op elk gewenst moment tussen het mobiele of vaste nummer. Zij wisselen dan het nummer dat de ontvanger van het gesprek ziet. Dat nummer kan bijvoorbeeld binnen uw organisatie een verkort intern nummer zijn.

Voicemail: De voicemail vanuit het mobiele netwerk komt te vervallen en wordt bij een Vast-Mobielintegratie verplaatst naar het Vast Bellen-platform. Indien gewenst kan de voicemail ook door de aangesloten telefooncentrale worden verzorgd. Dit kan bijvoorbeeld Cloud Communications Microsoft Teams, Mitel, Genesys Cloud of de eigen telefooncentrale van opdrachtgever zijn.

Doorschakelen: Het doorschakelen van alle gesprekken kunnen medewerkers activeren in de MijnGesprekapp. Hierbij kunnen zij vaste en mobiele nummers opgeven om naar door te schakelen. Er gelden uitzonderingen en beperkingen op het doorschakelen naar 0800- en 090xnummers en bepaalde internationale nummers.

Partij 3: Inschrijver begrijpt deze vraag niet geheel. Het betreft hier immers de aanbesteding voor vaste telefoniediensten. Er is een bewuste keuze gemaakt door de rijksoverheid om mobiel en vast in separate percelen/aanbestedingen uit te vragen. Wellicht is het in deze fase niet meer opportuun, echter Inschrijver is van mening dat een volledige vast-mobiel integratie met alle functionaliteiten pas mogelijk is wanneer zowel mobiel als vast bij 1 provider zijn ondergebracht.

Partij 4: Ons bedrijf kan Vast op Mobiel leveren als aanvulling op een UC-oplossing. Hiermee komt de mobiele presence beschikbaar in het UC/CC platform en kan de gebruiker uitbellen met een vast nummer vanaf de native dialer van zijn feature of smartphone. Dit past in een beweging in de markt waarbij kantoormedewerkers niet worden voorzien van een UC oplossing zoals Teams phone maar alleen met het mobiele toestel werken. Door de netwerk presence integratie is hun presence toch zichtbaar voor collega's in het contact center. Daarnaast kunnen ze een vast nummer presenteren als ze uitbellen wat voor sommige functies erg prettig kan zijn (sociaal domein, handhaving etc). Tot slot kunnen wij op de SBC een doorschakeling activeren waardoor oproepen naar bepaalde vaste nummers meteen worden doorgeschakeld naar het mobiele nummer van de gebruiker, zoals vastgelegd in de AD van de deelnemer. Hierdoor is geen UC licentie benodigd voor deze gebruiker maar blijft die toch bereikbaar op zijn vaste nummer. Door bovenstaande oplossing is een veel minder grote implementatie benodigd van de UC omgeving en kan die feitelijk beperkt blijven tot een Call Center oplossing voor Contact Center groepen en een telefonisten oplossing. Vergeleken met Operator Mobile Connect van Microsoft is deze oplossing ook veel flexibeler naar de eindgebruiker doordat een onderscheid mogelijk blijft tussen vast (zakelijk) en mobiele (zakelijk/privé) bereikbaarheid, de reden waarom veel organisatie van Forced on PBX (FoPBX) af willen. Operator Mobile Connect is feitelijk een stap terug naar FoPBX. Goede integratie tussen mobiel en vast vereist (op dit moment) dat beide nummers, zowel vast als mobiel, gebruik maken van hetzelfde onderliggende netwerk. Gezien de contract structuur van de IWR aanbestedingen is dat op dit moment het grootste struikelblok voor volledige integratie tussen vast en mobiel.

11b	Wat zijn naar uw deskundige mening de voor- en nadelen van ieder van de door u onder vraag 11a benoemde functionaliteiten?
------------	---

Partij 1: Door verkeer tussen zakelijk en mobiel te scheiden op de smartphone/ tablet op app niveau behoudt de gebruiker de vrijheid om een scheiding tussen zakelijk en privé verkeer te maken. Op het moment dat zakelijk verkeer volledig in de native dialer via een provider is geregeld heeft de provider hiermee een grotere lock-in verkregen wat laten wisselen van provider bemoeilijkt. Door zakelijk verkeer via een app af te handelen en deze gedeeltelijk te integreren met de local dialer kan een organisatie vrij makkelijk van mobiele provider wisselen zonder verlies aan zakelijke telefoniefunctie die een andere provider mogelijk niet ondersteunt.

Partij 2: De belangrijkste voordelen zijn grotere bereikbaarheid, professionelere uitstraling door vanaf mobiele telefoon uit te bellen met het vaste nummer van de opdrachtgever. Daarnaast ook een betere scheiding werk en privé door het kunnen uitschakelen van het vaste nummer op de mobiele telefoon. Belangrijkste nadeel is dat het aanpassing vraagt van de wijze van communiceren en dat je dit in een app moet instellen. Je moet dus nadenken over hoe en met welk nummer je bereikbaar wilt zijn en dat vergt aanpassing en adoptie van medewerkers.

Partij 3: Zie bovenstaand antwoord.

Partij 4: Het nadeel van bovenstaande oplossing is dat kantoormedewerkers die geen UC profiel meer hebben elkaars presence niet kunnen zien in de native dialer op hun mobiele toestel. In hun Teams app op de mobiel of laptop overigens wel. De Teams app kan door iedereen gewoon gebruikt worden voor alle andere functies zoals elkaar bellen via Teams, Teams meetings en collaboration alleen niet voor bellen naar vaste nummers of gebeld worden door vaste nummers.

12a	Wat zijn in uw netwerk de mogelijkheden om naast routeren van Nederlands georiënteerde publieke nummerblokken (E164) ook internationale/buitenlandse nummerblokken ten behoeve van inkomend verkeer aan te kunnen bieden? Bijv een +44 nummer afleveren op een locatie in NL. Denk hierbij aan Nederlands ambassades.
	Partij 1: Ons platform zit in meerdere landen in Europa. Het platform zelf kan nummers van het ene land laten binnen komen in het andere land. Soms zitten daar wel voorwaarden en wetgeving van de lokale landen aan vast. Afhankelijk van die regelgeving (bijvoorbeeld verplicht een kantoor in dat land hebben) is het mogelijk om een buitenlandsnummer in Nederland te laten landen als ook te gebruiken voor uitgaande nummer herkenning. Partij 2: In samenwerking met een partner met internationale footprint biedt respondent de dienst International SIP trunking aan. Hiermee kan opdrachtgever buitenlandse nummerblokken aanbieden in veel landen in de wereld waarbij het spraakverkeer uit het buitenland wordt afgehandeld op locaties in Nederland. Dit kan via het datanetwerk van de opdrachtgever of met gebruikmaking van de eigen verbindingen. Partij 3: Inschrijver biedt deze mogelijkheid op dit moment niet. In samenwerking met een partner is een maatwerkoplossing bespreekbaar waarin buitenlandse nummers worden geconfigureerd. Het betreft hier internationale trunks waarop niet dezelfde rapportages en beschikbaarheid van toepassing zijn als op nationale trunks. Partij 4: Op dit moment routeren wij geen internationale of buitenlandse nummerblokken naar een locatie in Nederland. Het hosten van buitenlandse nummerblokken is momenteel ook geen onderdeel van onze dienstverlening. Er zijn partijen in de markt aanwezig die dergelijke dienstverlening leveren in combinatie met servicenummers.
12b	Wanneer dat kan, kunt u dan svp uitleggen hoe het routeren van buitenlandse nummerblokken functioneel werkt en welke additionele zaken (zoals bijv. kostenregistratie en beschikbaarheid van de dienst) belangrijk zijn?
	Partij 1: Deze nummers komen op de gemeenschappelijke SIP trunk die het platform heeft aan en wordt vanuit daar gerouteerd naar de juiste Tennant en gebruiker. Partij 2: De functionele werking van de routing van buitenlandse nummerblokken is afgebeeld in onderstaande figuur: Dit geeft de routing weer van internationale SIP-trunk naar klant SBC (via VPN). In het wolkje van Internationaal SIP trunk zitten de geografisch gescheiden SBC's (Amsterdam-Londen). Deze SBC's routeren het SIP-verkeer van land van herkomst naar de SBC van de klant in Nederland, of naar ons eigen managed SBC. De internationale SIP trunks kun je afnemen als 1 trunk voor alle landen, of per land één trunk. Het is ook mogelijk om per land een back-up trunk af te nemen voor een hogere beschikbaarheid. De nummerblokken van de buitenlandse infrastructuur worden gemigreerd naar de internationale SIP trunk infrastructuur. Eindgebruikers die ontsloten zijn via het internet, maar onderdeel zijn van een buitenlands kantoor, worden d.m.v. van hun landcode gerouteerd via internationale SIP trunk naar hun eigen lokale vaste telefonie infrastructuur (daardoor zijn de gesprekken van desbetreffende landen lokale gesprekken en worden 112 oproepen lokaal afgehandeld). International SIP trunking maakt gebruik van bestaande connectiviteitsmogelijkheden. Denk hierbij aan VPN of over publiek internet rechtsreeks naar een Telefooncentrale of een Session Border Controller. De beschikbaarheid tussen de PoP's is 99,999%. End-to-end beschikbaarheid is 99,9%. Het kostenmodel kent een prijs voor de SIP trunks, bandbreedte, aantal nummers en het verbruik dat wordt afgerekend o.b.v. land van bestemming en het land van waaruit

wordt gebeld. Er is een aparte facturering van de belkosten van deze internationale SIP trunks.

Partij 3: Buitenlandse nummers kunnen gerouteerd worden door partijen met een licentie in het land waar het betreffende nummer zijn oorsprong vindt. Inschrijver heeft contracten met diverse partners die voor verschillende landen beschikken over dergelijke licenties. Buitenlandse trunks worden op een separate verbinding afgeleverd bij klanten. Afhankelijk van het land zijn hieraan kosten verbonden voor het aantal kanalen en gesprekken. Voor uitgaande gesprekken dient in de meeste gevallen uitgegaan te worden van internationale tarieven. Beschikbaarheid en rapportage mogelijkheden op dergelijke trunks zijn geen onderdeel van de standaard tooling.

Partij 4: Verkeer naar buitenlandse nummerblokken wordt op basis van de landencode gerouteerd. Hierbij gebruikt ons bedrijf Business LCR (least cost routing) in combinatie met een keuze op basis van gesprekskwaliteit. Indien mogelijk worden buitenlandse gesprekken onnet gerouteerd via partners zoals LG en onze groepsmaatschappij.

13	In principe wordt door opdrachtgever gezocht naar dienstaanbod volgens een (non-blocking) model met concurrent use/ gelijktijdige gesprekken. Geef svp een beschrijving van uw aangeboden dienstmodel? Staat dit model toe om ook "non blocking" te garanderen? Met andere woorden; dat er voor opdrachtgever altijd voldoende (inkomende én uitgaande) gesprekscapaciteit is?
-----------	---

Partij 1: Garantie kan worden gegeven dat die er altijd is. Zoveel gebruikers er in het systeem zijn zoveel gesprekken kunnen er gevoerd worden en voor de buitenlijnen is er altijd een overcapaciteit.

Partij 2: Onze dienst is een cloud oplossing die opgeschaald kan worden tot meer dan 10.000 SIP-kanalen. Hierdoor kan er een non-blocking oplossing geboden worden. In de praktijk gaat ons bedrijf in overleg met opdrachtgever over het gewenste gebruik en piekbelasting. Op basis van de piekbelasting zal de capaciteit van de dienstverlening worden bepaald en een commercieel aanbod worden gedaan voor het daadwerkelijk gebruik van de dienst. Vanzelfsprekend wordt daarin balans gebracht tussen deze piekbelasting en het ideale aantal concurrent users.

Partij 3: Het aantal kanalen dat beschikbaar is op een verbinding is zowel bij de operator als bij de klant geconfigureerd, en dient voor correcte werking gelijk te zijn. Het aantal beschikbare kanalen is in principe een softwarematige instelling die relatief eenvoudig en snel verhoogd kan worden. Limitatie hierin vormt de beschikbare bandbreedte op de access verbinding.

Het is niet mogelijk om dynamisch het aantal kanalen aan te passen; het is wel mogelijk om dit met beperkte doorlooptijd te doen. Aangezien licentiemodellen van trunks, PBX en overige componenten veelal kanaal gebaseerd zijn, verdient het de aanbeveling het aantal kanalen niet onnodig hoog te realiseren. Tijdens service meetings kan het aantal in gebruik zijnde kanalen gemonitord worden en indien van toepassing aangepast.

Inschrijver prefereert uitvraag op basis van aantallen gewenste kanalen boven uitvraag op basis van bandbreedte zoals dit nu in IWR2018 van toepassing is.

Partij 4: De grootte van de SIP trunk die wij aanbieden bepaald hoeveel gelijktijdige gesprekken mogelijk zijn. Hiernaast is het aantal CAPS (Call Attempts Per Second) bepalend voor de kans op congestie in het netwerk. De dimensionering van ons netwerk en de proactieve monitoring zorgen ervoor dat de kans op congestie in de praktijk niet voorkomt. Onze standaarddienst gaat uit van aantal Mb's per SIP Trunk, die bepalen hoeveel gesprekken er gelijktijdig kunnen plaatsvinden (100mb = ca. 1.000 gelijktijdige gesprekken). Echter vanuit kostenefficiëntie is het ook mogelijk om een model te creëren die uitgaat van het maximaal aantal mogelijke gelijktijdige gesprekken per verbinding. De SIP licenties zijn het meest dure onderdeel van de SIP dienst. Door het gebruik

hiervan te beperken is het mogelijk om de dienst tegen lagere kosten te leveren. Dit kan bijvoorbeeld in staffels:

- Van 0 tot 100 SIP kanalen: per 10 kanalen
- Van 100 tot 200 SIP kanalen: per 20 kanalen
- Van 200 tot 500 SIP kanalen: per 50 kanalen
- Van 500 tot 1000 SIP kanalen: per 100 kanalen
- Boven 1000 SIP kanalen : maatwerk

14	Video bellen is eigenlijk niets meer dan video toevoegen aan een audio gesprek. Afhankelijk van het gebruikte device of applicatie suite zou video- of beeldbellen los van een platform als Webex of Microsoft toegevoegd kunnen worden. Kunt u svp toelichten of beeldbellen en de daarmee samenhangende video CODEC-onderhandeling (nu of in de komende jaren) door uw netwerk ondersteund (zullen) worden?
-----------	--

Partij 1: UNIVERGE BLUE MEET Video Conferencing is een krachtige online vergaderoplossing die is ontwikkeld voor bedrijven van elke omvang. Onze gebruiksvriendelijke vergaderervaring is beschikbaar op desktop en mobiele apparaten, zodat u overal en altijd betrouwbare, stressvrije vergaderingen kunt houden. Met de hoogste HD audio- en videokwaliteit, interactieve samenwerkingstools en kunstmatige intelligentie-mogelijkheden, transformeert u communicatie tot een slimmere, snellere, boeiende en veilige, bruikbare vergaderervaring.

Partij 2: In de komende jaren wordt de mogelijkheid tot beeldbellen en de daarmee samenhangende video CODEC-onderhandeling door ons netwerk ontwikkeld en ondersteund. Er zal dan sprake zijn van een video-codec in het SIP bericht van/naar PSTN-nummers.

Partij 3: Het is correct dat SIP in principe zowel voor Voice als Video toegepast kan worden, mits de juiste codec onderhandeld wordt tijdens het opzetten van de verbinding. PSTN netwerken zijn echter ingericht op basis van spraak, en niet op basis van Video. Ook de benodigde bandbreedte op de access en overige componenten is afgestemd op spraak, evenals de PBX waarde lijnen op termineren. In de praktijk zien we dus PSTN als spraak only netwerk.

Partij 4: In de basis ondersteunt het netwerk van ons bedrijf allerlei media die via SIP onderhandeld wordt. Op dit moment ondersteunen wij voice codecs (OneFixed), mobiele voice codecs (VoLTE), maar het kan ook video codecs ondersteunen. Op dit moment zijn er geen diensten beschikbaar waarbij videocodecs ondersteund worden. Het is mogelijk dat in de toekomst dit soort diensten ontwikkeld worden.

15	Geef svp een toelichting wat voor opdrachtgever verder nog relevante mogelijkheden en visies vanuit uw organisatie zijn voor nieuwe dienstverlening in de komende vijf jaar?
-----------	---

Partij 1: De komst van 5G voor mobiele communicatie gaat er voor zorgen dat steeds sneller en veiliger kan worden uitgewisseld. Daarnaast zien we dat de jongere generatie, die volledig met Smartphone opgroeit andere manieren van communicatie hanteert. Bellen via een app ipv native dialer zal steeds meer gemeengoed worden waarbij het gebruik van video ook een steeds grotere vlucht zal gaan nemen. In de tijd van corona is het topic bereikbaarheid voor een gedeelte overboord gegoooid. Doordat iedereen en overal thuis werkte en aangewezen was op doorschakelen van zakelijk naar privé om überhaupt bereikbaar te zijn waren de eisen aan telefonie tot het minimale beperkt van bellen en gebeld worden. De verwachting is dat dit in de toekomst weer anders zal moeten waarbij er steeds vaker eisen zullen worden gesteld dat een gesprek naar een medewerker binnen een bepaalde tijd op een bepaalde manier beantwoord moet zijn, ipv ergens in een voicemailbox te belanden en nooit meer te worden afgeluisterd.

Partij 2: De relevante mogelijkheden en visies vanuit ons bedrijf voor nieuwe dienstverlening in de komende vijf jaar zijn hieronder weergegeven.

De i-samenleving vraagt om 1 informatiegedreven en verbonden overheid

Het Nederland van de toekomst vraagt om een digitale, informatiegedreven samenleving waarin privacy, veiligheid, betrouwbaarheid, beschikbaarheid, duurzaamheid, efficiëntie en wendbaarheid belangrijker zijn dan ooit. Het is aan de overheid om de transformatie naar die samenleving te leiden.

Overheid als regisseur: Ons bedrijf gelooft in 1 informatiegedreven overheid die vergaande digitalisering faciliteert en realiseert, voor burgers, bedrijven en de overheid zelf. Met een gedeelde datagedreven infrastructuur van publieke en private netwerken die dit mogelijk maakt. De overheid is hierin de regisseur die de kaders stelt waarmee zij de ontwikkelingen in de politiek, samenleving, ICT en technologie bij elkaar brengt. Een overheid die richting geeft vanuit haar maatschappelijke verantwoordelijkheid. Het adagium hiervoor: 'gezamenlijk en gedeeld wat kan, afzonderlijk wat echt moet'.

Investeren in digitale infrastructuur: Wij investeren jaarlijks circa 1,1 miljard euro aan de uitrol van glasvezel in Nederland met als ambitie in 2026 circa 80 procent van de Nederlandse huishoudens aan te sluiten op haar netwerk. Daarmee versterken wij de positie van ons land als een leidend, innovatief en duurzaam digitaal knooppunt in de wereld. Een veilige en vertrouwde vestigingsplaats voor nationale en internationale bedrijven met een hoogwaardige, digitale maatschappelijke infrastructuur. Niet voor niets werkt bijna de helft van de ambtenaren met de publieke netwerken die ons bedrijf exploiteert en/of beheert, gebruiken bijna alle Nederlanders onze zichtbare én onzichtbare diensten en zijn we dé ICT-partner voor zo'n 30% van alle bedrijven in Nederland. We zijn ervan overtuigd dat goede ICT bijdraagt aan een schone, gezonde en welvarende wereld. En aan een samenleving waarin overheid, burgers en bedrijven op een veilige manier informatie kunnen uitwisselen. Daarom werken we samen met de overheid en andere marktpartijen aan duidelijke afspraken voor een slimme en robuuste informatiesamenleving, zodat burgers, bedrijven en ambtenaren nóg beter worden bediend en beschermd.

Veiligheid is cruciaal: Hybride werken is tegenwoordig de norm. Het biedt namelijk niet alleen de medewerkers binnen de overheid, maar ook de overheidsorganisaties veel voordelen. Om ook hybride optimaal samen te werken, wordt steeds meer gebruikgemaakt van 'as-a-service' cloudapplicaties. Hoewel deze gemakkelijk te gebruiken en te activeren zijn, neemt het gebruik ook veiligheidsrisico's met zich mee. Secure Connect zorgt ervoor dat overheidsorganisaties grip houden op de data en tegelijkertijd cloudapplicaties gebruikt worden. Zo kunnen overheidsmedewerkers veilig en zonder gedoe (cloud)applicaties gebruiken en op afstand werken. Goede ICT moet veilig zijn. Daarom toetst ons bedrijf zijn producten en diensten altijd aan de eigen Security Policy. Daarbij kijken we niet alleen naar de veiligheid van verbindingen, maar ook naar de waarborging van privacy en bedrijfsgevoelige informatie. Uiteraard voldoet ons bedrijf daarbij aan de hoogste securitystandaarden, zoals de ISO 27001.

Secure Connect voor extra veilig hybride werken: Met de Secure Connect dienst kunnen medewerkers aangeven welk apparaat of welke verbinding prioriteit heeft. Hierdoor wordt deze connectie geoptimaliseerd, waardoor programma's (via de cloud) beter en sneller werken. Ook zorgt Secure Connect ervoor dat beheerders inzage hebben welk toestel een verbinding maakt met het organisatienetwerk. Medewerkers kunnen op hun zakelijke apparaten ook privédingen doen, maar kunnen op privétoestellen niet zomaar alle zakelijke toepassingen gebruiken als je dit afschermt en inricht met Secure Connect. Secure Connect wordt standaard geleverd met Internet Security. Hiermee wordt niet alleen een veilige koppeling tussen uw medewerkers en uw (cloud)applicaties gerealiseerd, het bevat ook een aantal cybersecuritydiensten, zoals een Secure Web Gateway en een Cloud Access Security Broker. Met Internet Security heeft u zicht en controle op het gebruik van cloudapplicaties, ongeacht op welke locatie deze gebruikt worden. Onveilige applicaties worden herkend en kunt u op de zakelijke toestellen van uw medewerkers blokkeren. Ook wordt de toegang tot botnets en command-and-control-sites geblokkeerd. Zo zijn uw medewerkers beschermd tegen online gevaren zoals

phishing, malware en spam. En wil een medewerker een geblokkeerde applicatie alsnog gebruiken, dan kan dat gewoon via zijn privét toestel. Zo ervaren medewerkers geen beperkingen en loopt u geen risico's.

Extra veiligheid met Enterprise Mobility Management: Opdrachtgever kan met Enterprise Mobility Management vanuit één online beheerplatform alle toestellen beheren en het mobilitybeleid omzetten in concrete configuraties en policies voor overheidsmedewerkers. Fysieke toegang tot de mobiele apparaten is daarbij niet nodig. De oplossing van ons bedrijf reguleert de toegang tot privacygevoelige informatie en beveiligd de overheidsdata die op de devices staan. Voorbeeld: informatie beschikbaar op de OneDrive van uw organisatie kan niet worden gekopieerd naar de whatsapp desktopversie die uw medewerkers privé gebruiken.

Mobile Threat Defense: Geen enkel mobiel apparaat is standaard volledig beschermd tegen de nieuwste aanvalstechnieken van hackers, ongeacht het besturingssysteem. Mobile Threat Defense scant mobiele apparaten binnen uw bedrijfsnetwerk daarom op bekende en onbekende bedreigingen. De mobiele applicatie Mobile Threat Defense is gemakkelijk te installeren op ieder toestel binnen uw bedrijfsnetwerk en zeer eenvoudig in gebruik. Via een overzichtelijk portaal kunt u alle apparaten controleren op risico's. Op het moment dat bedreigingen worden gesignaleerd, krijgt u een melding. U ziet dan welke acties u stapsgewijs moet ondernemen. Deze dienst biedt bescherming op applicatie- en netwerkniveau. Secure Connect, EMM en Vast-Mobiel integratie, en Mobile Threat Defense kunnen gezamenlijk of separaat afgenomen worden.

Partij 3: Inschrijver heeft een partner strategie. In samenspraak met haar partners is een breed pallet aan complementaire diensten beschikbaar. Deze diensten stellen gebruikers in staat om steeds slimmer gesprekken te routeren naar de gewenste beantwoorder, zodat voorkomen wordt dat gebruikers moeten zoeken naar de juiste ingang. Het betreft hier maatwerk diensten.

Partij 4: In de komende vijf jaar verwachten wij veel ontwikkeling als het gaat om:

- Verdergaande implementatie van 5G-technologie: 5G biedt snellere internetverbindingen en lagere latentie dan 4G, en zal in staat zijn om een grotere hoeveelheid verbonden apparaten aan te kunnen. Dit zal leiden tot nieuwe toepassingen en diensten, zoals autonome voertuigen, internet of things en virtual reality.
 - Verdergaande groei van de cloud: Cloud-diensten zullen steeds belangrijker worden voor bedrijven en consumenten, en zullen leiden tot nieuwe zakelijke modellen en efficiëntere werkmethoden.
 - Toenemende adoptie van software-defined networking (SDN) en network functions virtualization (NFV): Deze technologieën stellen telecombedrijven in staat om hun netwerken efficiënter te beheren en flexibeler te maken, waardoor ze sneller kunnen reageren op veranderende eisen.
 - Toenemende adoptie van edge computing: Edge computing maakt het mogelijk om dataverwerking en -analyse dicht bij de bron te doen, wat leidt tot snellere reacties en minder bandbreedtegebruik.
 - Toenemende focus op beveiliging: Met de groei van het internet of things en de toenemende hoeveelheid verbonden apparaten, zal de beveiliging van deze apparaten en netwerken een grotere prioriteit worden.
- Specifiek op het gebied van vaste telefonie zien wij de volgende ontwikkelingen:
- Toenemende adoptie van Unified Communications (UC): UC integreert verschillende communicatiekanalen, zoals voice, video, instant messaging en e-mail, in één enkel platform. Dit zal de communicatie tussen medewerkers efficiënter maken en de productiviteit verhogen.
 - Toenemende focus op mobiele integratie: Met de groei van smartphones en tablets, zal de integratie van vaste telefonie met mobiele apparaten een grotere prioriteit worden. Dit zal leiden tot meer flexibiliteit voor gebruikers, waardoor ze gemakkelijk kunnen schakelen tussen verschillende apparaten en locaties.
 - Toenemende focus op beveiliging: Met de groei van cyberbedreigingen, zal de beveiliging van vaste telefonie-systemen een grotere prioriteit worden. Dit zal leiden tot meer geavanceerde beveiligingsmaatregelen, zoals encryptie en authenticatie.
 - Toenemende adoptie van AI (Artificial Intelligence) en automatisering: AI en automatisering zullen worden gebruikt om de efficiëntie van vaste telefonie-systemen te

verhogen en de kosten te verlagen. Dit leidt tot bijvoorbeeld automatisch antwoorden van de telefooncentrale en zelfbediening opties voor de klant.

16 Kunt u een Hosted Voice oplossing leveren?

Partij 1: Ja, onze oplossing is geheel hosted voice.

Partij 2: Ja, Ons bedrijf kan een Hosted Voice oplossing leveren op basis van Cloud Communications Mitel uit de Smart Combinations propositie. Alle andere oplossingen komen uit de cloud.

Partij 3: Ja, Inschrijver beschikt over een breed portfolio aan Hosted Voice oplossingen. Zowel Cloud PBX oplossingen, als integraties van diverse PBX-en en toepassingen, als netwerk intelligentie zijn onderdeel van het portfolio.

Partij 4: Ja. Wij hebben twee Hosted Voice oplossingen. One Net en Avaya Omnia.

17 Zo ja, kunt u deze dienst functioneel beschrijven?

Partij 1: Dit is een in de Cloud geboren SaaS-oplossing. Enkele van de redenen waarom deze zich onderscheidt in de markt zijn:

> Uptime en betrouwbaarheid: De betrouwbaarheid van NEC's UNIVERGE BLUE is van wereldklasse voor zowel spraak- als datadiensten en geeft invulling aan onze financieel gesteunde SLA van 99,999%.

> Klantondersteuning: Meerdere datacenters verhogen de betrouwbaarheid en minimaliseren vertragingen, 99,999% financieel ondersteunde uptime SLA, stringente eigen netwerktesttools en prekwalificatie richtlijnen zorgen voor een betrouwbare verbinding en 24/7 ondersteuning. U kunt met een gerust hart uw aandacht bij uw bedrijf houden.

> Complete UCaaS en CCaaS productsuite: NEC heeft een uitgebreide reeks UCaaS- en CCaaS-oplossingen die uitstekend voldoen aan de behoeften van bedrijven van elke omvang. De UNIVERGE BLUE-technologie stelt ons in staat om ons snel aan te passen aan veranderende vereisten van onze klanten.

Partij 2: Ons bedrijf levert een Hosted Voice oplossing op basis van Cloud Communications Mitel uit de Smart Combinations propositie. De dienst wordt vanuit de Nederlandse datacenters geleverd en is ingericht volgens de strenge security eisen van ons bedrijf. Deze cloudomgeving is specifiek voor u ingericht in ons datacenter. Hier zijn de verschillende toepassingen (o.a. MiVoice Business, MiCollab en MiContact Center) geïnstalleerd. Het ontsluiten van uw locaties naar het datacenter van ons bedrijf gaat via internet of een VPN verbinding. Het uitgangspunt is dat uw cloud-omgeving aangesloten wordt via onze dienst (SIP trunk). Het beheren (functioneel beheer) van uw omgeving vindt plaats via uw eigen management portal waarbij u maandelijks wordt gefactureerd voor het gebruik van de omgeving. Optioneel is het mogelijk het functioneel beheer van uw omgeving door ons bedrijf te laten verzorgen.

Cloud Communications Mitel biedt u de volgende functionaliteiten:

1. de centrale omgeving is ingericht op een multi-instance virtuele omgeving; deze virtuele omgeving wordt ingericht voor de Mitel applicaties uit de Mitel MiVoice Business Suite;
2. het technisch beheer van uw omgeving wordt door aanbieder verzorgd;
3. functioneel beheer via een portal;
4. Het gebruik van het aantal profielen en andere afgenomen functionaliteiten worden per maand in rekening gebracht; peildatum is de laatste dag van de maand;
5. een 24/7 Service Level Agreement (SLA);
6. gebruik van vaste toestellen, mobiele toestellen en softphones.

Partij 3: Verwijst naar bijlagen met dienstbeschrijvingen.

Partij 4: One Net is een UCaaS oplossing met een zeer goede vast mobiel integratie. Mobile gebruikers met gemiddelde UC eisen zijn de norm waarbij er wel een goede integratie is met vaste telefonie. De eerder beschreven Vast op Mobiel propositie is onder water een afgeleide van onze One Net propositie. One Net is niet goed in klantspecifieke integraties met bijvoorbeeld een AD of een CRM applicatie (read only). Ook is de CC module beperkt tot huntgroepen en basale rapportages. De uitrol van One Net gaat erg makkelijk en kent door de grote mate van standaardisatie een goed prijsniveau

vergeleken met andere UCaaS oplossingen. Avaya Omnia is een UCaaS oplossing die vooral geschikt is voor grote organisaties die veel klant specifieke wensen hebben qua integraties, een hele hoge beschikbaarheid eisen en een geïntegreerd CC nodig hebben met uitgebreide functies en rapportages.

CONCEPT