



Logius
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Specificatie van de Prestatie

Aanbesteding Koppelnets Publieke Sector (KPS)

Versie 1.0a

Organisatie Logius
Datum 11 juni 2019
Status Definitief

Inhoud

Inhoud.....	2
Colofon	3
1. Inleiding	4
1.1. <i>Over dit document.....</i>	4
1.2. <i>Aanleiding</i>	4
1.3. <i>Doel en doelgroep</i>	4
1.4. <i>Leeswijzer</i>	4
1.5. <i>Verantwoording.....</i>	4
2. Beschrijving Diginetwerk en het huidige KPS	5
3. Eisen en wensen	8
3.1. <i>Toelichting.....</i>	8
3.2. <i>De dienst.....</i>	8
3.3. <i>Het beheer</i>	12
3.4. <i>De locatie</i>	16
3.5. <i>Duurzaamheid.....</i>	16
3.6. <i>De migratie.....</i>	17
3.7. <i>Innovatie.....</i>	18
Begrippen en afkortingen	22

Colofon

Documentnaam	Bijlage 3 - Specificatie van de Prestatie KPS
Versienummer	1.0a
Organisatie	Logius Postbus 96810 2509 JE Den Haag

1. Inleiding

1.1. Over dit document

Dit document bevat de Specificatie van de Prestatie voor de aanbesteding van het Koppelnets Publieke Sector (KPS). Het doel van dit document is om de gevraagde functionaliteit van de dienst te beschrijven en te vertalen in eisen en wensen, zodat inschrijvers in staat zijn een inschrijving te kunnen doen voor deze opdracht.

In opvolging van de marktconsultatie die eind vorig jaar heeft plaatsgevonden, is in deze Specificatie van de Prestatie het advies van de marktpartijen meegenomen, voor zover dit de belangen en de ideeën van Logius niet schaadt.

1.2. Aanleiding

Het tactisch en operationeel beheer van het KPS wordt momenteel in opdracht van Logius uitgevoerd door Bureau Ketenbeheer Werk en Inkomen (BKWI). BKWI heeft hierbij het technisch beheer en housing van het KPS uitbesteed aan commerciële leveranciers. BKWI heeft aangegeven het beheer van het KPS niet langer te zullen uitvoeren, omdat dit niet tot haar kerntaken behoort. Logius heeft daarop besloten om de realisatie en het beheer van KPS aan te besteden.

1.3. Doel en doelgroep

Het doel van het document is het weergeven van de gevraagde functionaliteiten van het Koppelnets Publieke Sector, zoals deze dienst aanbesteed wordt en als dienst gebruikt kan worden door de (Rijks)overheid.

Dit document is bedoeld voor marktpartijen die het KPS als dienst kunnen leveren. De dienst is niet opgebouwd uit percelen en dient als één geheel aangeboden te worden.

1.4. Leeswijzer

Hoofdstuk 1 vormt de inleiding van de aanbesteding. Hoofdstuk 2 bestaat uit de beschrijving van het huidige KPS. Hoofdstuk 3 bestaat uit de Specificatie van de Prestatie onderverdeeld in verschillende rubrieken. Als inleiding van een rubriek wordt eerst de functionele vraag beschreven en daarna per item in tabelvorm uitgevraagd. Aan het eind van dit document is een verklarende woordenlijst opgenomen.

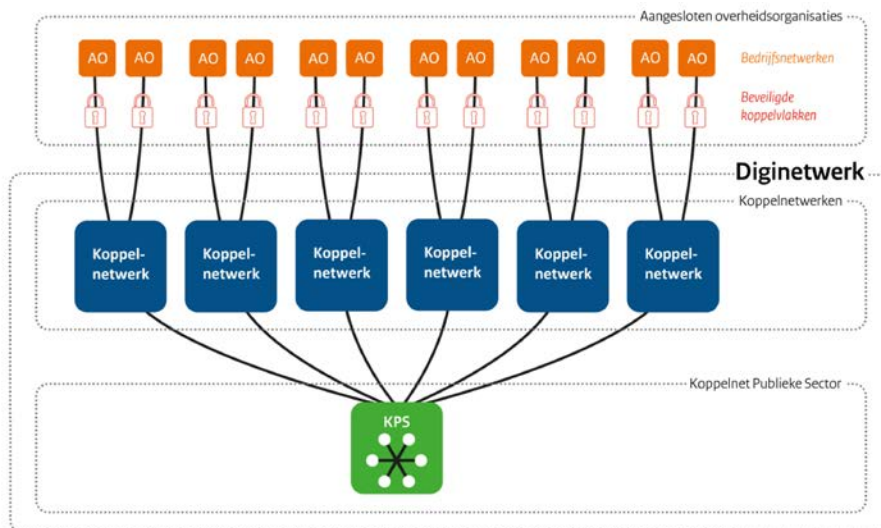
1.5. Verantwoording

Dit document is gebaseerd op inhoudelijke bijdragen van het merendeel van de aangesloten koppelnetswerkbeheerders en van Logius. Dit document is beschreven aan de hand van de huidige dienstverlening, de toekomstige wensen en eisen en de actuele beveiligingsstandaarden (BIR/BIO/ISO).

2. Beschrijving Diginetwerk en het huidige KPS

Diginetwerk is een afsprakenstelsel voor het koppelen van besloten netwerken van de overheid. Het doel van Diginetwerk is om een veilige, efficiënte en effectieve standaardoplossing te bieden voor elektronische gegevensuitwisseling tussen organisaties die een taak vervullen in de publieke sector. Diginetwerk biedt de connectiviteit waarmee elke organisatie binnen het publieke domein elke andere organisatie daarbinnen kan bereiken, op eenvoudige en gestandaardiseerde wijze via geharmoniseerde en in samenhang gekoppelde besloten netwerken en zonder afhankelijkheid van internet.

Diginetwerk is een besloten netwerk van netwerken waarop alle Nederlandse overheidsorganisaties kunnen aansluiten. Diginetwerk is op dit moment samengesteld uit negen koppelnetwerken. De koppelnetwerken sluiten de op Diginetwerk aangesloten organisaties aan. Voorbeelden van aangesloten organisaties zijn: gemeenten, organisaties met een publieke taak, Rijksoverheden en semi-overheden. De koppelnetwerken zijn onderling gekoppeld via het Koppelnets Publieke Sector (KPS). Het KPS wordt momenteel in opdracht van Logius door BKWI beheerd, waarbij Quanza Engineering in opdracht van BKWI de technische uitvoering verzorgt en KPN de housing.



figuur 1: Diginetwerk

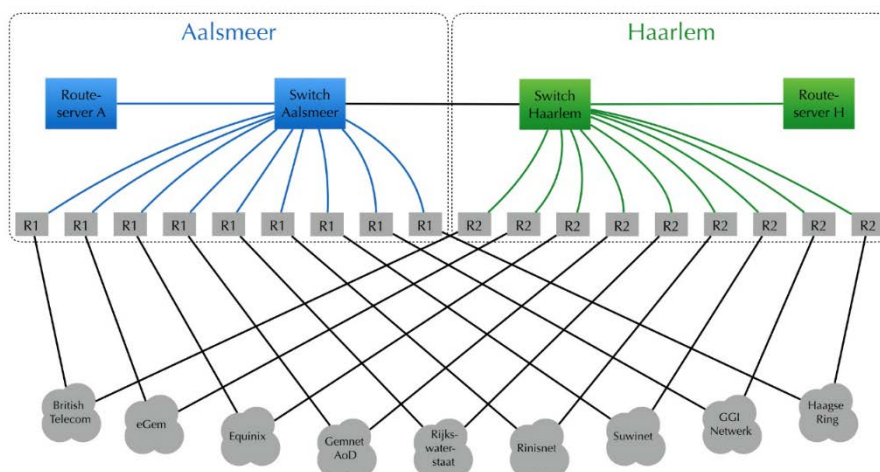
Het KPS is dubbel uitgevoerd en bevindt zich op twee locaties:

KPN Datacenter Aalsmeer
Lakenblekerstraat 13
1431 GE Aalsmeer

KPN Datacenter Haarlem
A. Hofmanweg 1
2031 BH Haarlem

In beide datacenters neemt BKWI drie kasten af. In twee hiervan kunnen de koppelnetwerk-leveranciers de apparatuur plaatsen waarmee zij koppelen aan het KPS. In de derde kast staat de apparatuur van het KPS zelf. De apparatuur van het KPS bestaat uit één of meerdere ethernetswitches, een routeserver en apparatuur voor monitoring en beheer.

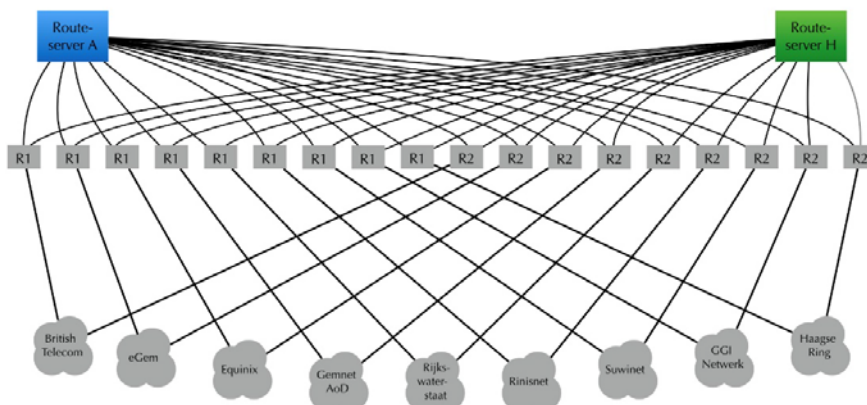
De switches op beide locaties zijn op laag 2-niveau gekoppeld. Ieder koppelnetwerk sluit op beide locaties een router op de KPS-switch aan. Zie figuur 2.



figuur2: Fysieke inrichting huidige KPS

In figuur 2 is de apparatuur van de twee KPS-locaties in respectievelijk blauw en groen aangegeven. De in grijs weergegeven apparatuur wordt beheerd door de leverancier van elk koppelnetwerk.

De routers van de koppelnetwerken onderhouden ieder een BGP-sessie met de routeservers op beide locaties, zie figuur 3.



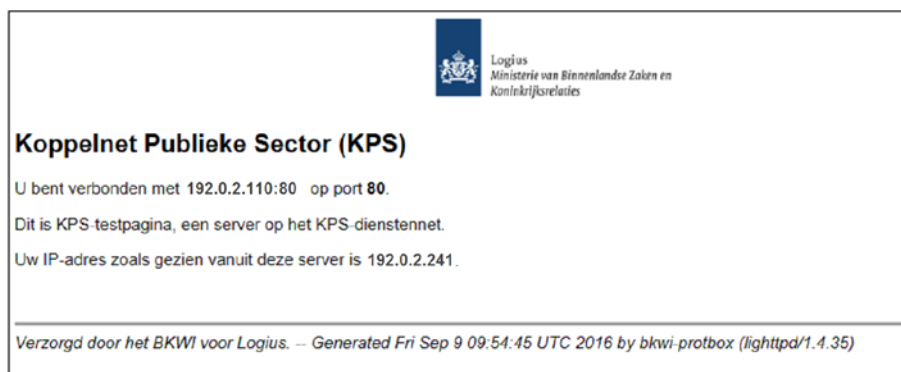
figuur3: BGP-sessies huidige KPS

Elke koppelnetwerkrouter adverteert de prefix(en) van het betreffende koppelnetwerk naar beide KPS-routeservers, en de routeservers distribueren alle prefixen van de gezamenlijke koppelnetwerken naar de routers van de koppelnetwerken.

De routers van de koppelnetwerken onderhouden geen BGP-sessies met routers van andere koppelnetwerken. Verkeer tussen twee koppelnetwerken wordt via de KPS-switch tussen de routers van deze koppelnetwerken uitgewisseld.

De KPS-routeservers passen filters toe die alleen de Diginetwerk-prefixen doorlaten. Tevens passen de KPS-routeservers voorkeur toe door het gebruik van de BGP MED om verkeer tussen de koppelnetwerken in eerste instantie via de locatie Aalsmeer te laten lopen. Mocht een koppelnetwerk niet beschikbaar zijn in Aalsmeer, dan is de tweede voorkeur om verkeer van/naar dat koppelnetwerk in Haarlem af te handelen. Pas in laatste instantie zal het verkeer tussen de router van het ene koppelnetwerk in Aalsmeer en de router van het andere koppelnetwerk in Haarlem afgehandeld worden via de koppeling tussen de switches van twee KPS-locaties.

Op het KPS is een test-website beschikbaar, waar een http-sessie naartoe kan worden gemaakt. Deze site geeft het IP adres terug van de initiator. De pagina van de testsite is in onderstaande figuur weergegeven.



figuur 4: KPS test-website

Logius heeft in de aangesloten koppelnetwerken testpunten opgenomen die continu bewaakt worden. Dit is zichtbaar gemaakt met behulp van de Uptrends Infra-applicatie.

Binnen Diginetwerk worden adresblokken van een klein aantal publieke IPv4- adresreeksen gebruikt. Deze adressen worden door Logius aan de koppelnetwerken en individuele aangesloten organisaties uitgegeven.

Op korte termijn zal tevens IPv6 geïmplementeerd worden in koppelnetwerken. Aangesloten organisaties zullen met specifieke IPv6-adresblokken binnen het overheidsbrede IPv6-nummerplankader aansluiten op Diginetwerk. IPv6-adresruimte binnen het overheidsbrede IPv6-nummerplankader, waaronder IPv6-adresruimte voor niet-overheden die diensten verlenen aan overheidsorganisaties via diginetwerk, wordt door Logius uitgegeven.

Meer informatie over het huidige Diginetwerk is terug te vinden op de website van Logius: <https://www.logius.nl/diensten/diginetwerk>.

3. Eisen en wensen

3.1. Toelichting

De Specificatie van de Prestatie onderscheidt eisen en open vragen:

Eis: Aan eisen dient voldaan te worden. Voldoet de Wederpartij niet aan de eis, dan vervalt zijn inschrijving. De eisen zijn geldig gedurende de gehele contractperiode.

Een eis is weergegeven als 'Eis xx'.

Vraag: De Wederpartij wordt gevraagd om een beschrijving, ontwerp of plan aan te leveren bij het betreffende vraagpunt. Aan een gegeven antwoord wordt een score gegeven.

Een vraag is weergegeven als 'V xx'.

De eisen en vragen zijn geclusterd in de volgende categorieën, die samen de totale gevraagde dienstverlening omvatten:

- De dienst - de inrichting van het KPS.
- Het beheer - het operationeel en tactisch beheer van het KPS.
- De locaties van het KPS.
- Duurzaamheid.
- De migratie – de migratie van het KPS.
- Innovatie – de realisatie van doorontwikkeling van het KPS.

3.2. De dienst

De gevraagde dienstverlening bestaat functioneel uit een contract met één leverancier die Logius "ontzorgt" voor het koppelen van de verschillende koppelnetwerken via een KPS en het operationeel houden van dit knooppunt en het handhaven van de Aansluitvoorwaarden KPS.

De dienstverlening dient schaalbaar te zijn qua aantal aangesloten koppelnetwerken en qua volume van dataverkeer. We vragen een beschikbaarheid van minimaal 99,9% up-time per locatie zodat de dienst altijd functioneert. Het niet of onvoldoende functioneren van de dienst zal direct landelijk invloed hebben op een groot aantal primaire processen en een zeer groot aantal medewerkers binnen en buiten de gehele overheid treffen. Gezien de hoge mate van beschikbaarheid dient het KPS over minstens twee onafhankelijke locaties verspreid te zijn, waarbij het risico van uitval zoveel mogelijk geminimaliseerd dient te zijn.

Op dit moment zijn 9 koppelnetwerken aangesloten, maar in de toekomst kunnen dit er meer of minder worden. De bandbreedte en aansluitpunten moeten kunnen groeien met de groei van de verkeerstromen over het KPS.

Diginetwerk is aangewezen als vitale voorziening voor Nederland. Daarmee is KPS, als essentieel onderdeel van Diginetwerk, een vitale voorziening. Dit betekent dat KPS valt onder de Wet Beveiliging Netwerk

en Informatiesystemen (Wbni) en dat de uiteindelijke aanbieder van KPS een zogeheten aanbieder van essentiële diensten is (AED).

Bij vitale diensten gaat er extra aandacht uit naar de bescherming van de vitaliteit hetgeen zich vertaalt naar continuïteit, integriteit en vertrouwelijkheid.

Ref.	Omschrijving
Eis 1	De Wederpartij is leverancier van essentiële diensten (AED) voor KPS in het kader van de Wbni en voldoet per productiedatum aan deze wet en de bijbehorende uitvoeringsverordening EU 2018/151-artikel 2. De meld- en zorgplicht zijn daarmee van toepassing op de te leveren dienst. Zie: • https://www.rijksoverheid.nl/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk--en-informatiesystemen-Wbni-voor-digitale-dienstverleners • https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32018R0151&from=EN
V1	Zorgplicht: Welke concrete maatregelen, heeft de Wederpartij genomen of gaat hij voor de productiedatum nemen als AED voor het leveren en garanderen van de KPS dienst gedurende de looptijd? Neem hierbij ook op welke maatregelen getroffen worden om Eis 39 in te vullen. Antwoord V1:
V2	Meldplicht: Hoe heeft de Wederpartij de meldplichtprocedures conform Wbni ingeregeld of gaat hij per start van de in productienamen uitvoeren als AED voor het leveren en garanderen van de KPS dienst gedurende de looptijd? Antwoord V2:
Eis 2	De Wederpartij is en blijft gedurende de looptijd gevestigd in de EU, waarbij ook de gevraagde dienstverlening vanuit de EU plaatsvindt en blijft plaatsvinden.
Eis 3	De Wederpartij levert als dienst de implementatie van het KPS waarop koppelnetwerken worden aangesloten, inclusief het beheer, migratie aan het begin en het einde van het contract, innovatie van het KPS en alle bijbehorende zaken die van een dienst verwacht mogen worden.
Eis 4	De Wederpartij levert minimaal het huidige aantal aansluitingen (11) met de bijbehorende bandbreedte (100 Mb & 1 Gb), zodat koppelnetwerken kunnen migreren op basis van hun huidige koppelvlak om hun migratiekosten te minimaliseren.
Eis 5	De Wederpartij levert een schaalbare dienst, zowel in aantal aansluitingen als in bandbreedtes. Deze twee aspecten moeten onafhankelijk van elkaar kunnen worden geschaald.
V3	Geef aan wat de schaalbaarheid is van het KPS met betrekking tot bandbreedte en aansluitmogelijkheden per locatie. Antwoord V3:

Ref.	Omschrijving
Eis 6	De beschikbaarheid van de dienst KPS is per locatie minimaal 99,9 % gemiddeld op jaarbasis.
V4	Licht toe aan de hand van een berekening en een onderbouwing hoe beschikbaarheid (Eis 6) per locatie van de dienst KPS gegarandeerd wordt en hoe dit resulteert in de totale beschikbaarheid van de dienst.
	Antwoord V4:
V5	De AIVD vindt in haar jaarverslag 2018 het onwenselijk dat Nederland voor de uitwisseling van gevoelige informatie of voor vitale processen afhankelijk is van de hard- of software van bedrijven uit landen waarvan is vastgesteld dat ze een offensief cyberprogramma tegen Nederlandse belangen voeren. De Wederpartij wordt gevraagd aan te geven hoe hij hier invulling aan denkt te geven.
	Antwoord V5:
Eis 7	De Wederpartij garandeert dat buitenlandse mogendheden niet op grond van een MLAT (mutual legal assistance treaty) of andere vorm van wetgeving of via zeggenschap in de onderneming van de Wederpartij toegang hebben tot de gegevens of de continuïteit van de dienstverlening kunnen beïnvloeden. Bij twijfel of zal kunnen worden voldaan aan het gestelde kan er een veiligheidsonderzoek worden gestart, conform de Wet Veiligheidsonderzoeken.
Eis 8	De dienst is zodanig ingericht dat koppelnetwerken aangesloten kunnen worden conform de aansluitvoorwaarden https://www.logius.nl/sites/default/files/public/bestanden/diensten/DigiNetwerk/Aansluitvoorwaarden-Koppelnets-Publiek-Sector_1.pdf .
Eis 9	De dienst is ingericht conform de architectuurbeschrijving van Diginetwerk, zoals beschreven op de website van Logius: https://www.logius.nl/diensten/diginetwerk

Ref.	Omschrijving												
Eis 10	De dienst voldoet aan de volgende service voorwaarden: <table border="1"> <tr> <td>Oplossen van incidenten</td><td>24 x 7</td></tr> <tr> <td>Proactief beheer</td><td>24 x 7</td></tr> <tr> <td>Maximale Reactietijd (telefonisch) Proactief beheer</td><td>5 minuten</td></tr> <tr> <td>Boete verstoring gehele dienst</td><td>€ 10.000,- per 15 minuten</td></tr> <tr> <td>Verdubbeling boete</td><td>Bij 2^e en volgende verstoringen (sliding window*)</td></tr> <tr> <td>Korte onderbrekingen** (< 5 min.)</td><td>Max. 2x per jaar ongecontroleerd. (Gecontroleerd in overleg)</td></tr> </table> * sliding window van 1 jaar = per aaneengesloten periode van 365 dagen ** Geldt ook voor onderbrekingen als gevolg van overschakelen tussen primaire en secundaire apparatuur of locatie.	Oplossen van incidenten	24 x 7	Proactief beheer	24 x 7	Maximale Reactietijd (telefonisch) Proactief beheer	5 minuten	Boete verstoring gehele dienst	€ 10.000,- per 15 minuten	Verdubbeling boete	Bij 2 ^e en volgende verstoringen (sliding window*)	Korte onderbrekingen** (< 5 min.)	Max. 2x per jaar ongecontroleerd. (Gecontroleerd in overleg)
Oplossen van incidenten	24 x 7												
Proactief beheer	24 x 7												
Maximale Reactietijd (telefonisch) Proactief beheer	5 minuten												
Boete verstoring gehele dienst	€ 10.000,- per 15 minuten												
Verdubbeling boete	Bij 2 ^e en volgende verstoringen (sliding window*)												
Korte onderbrekingen** (< 5 min.)	Max. 2x per jaar ongecontroleerd. (Gecontroleerd in overleg)												
V6	De Wederpartij dient een ontwerp van de dienst, zoals deze door Wederpartij geleverd gaat worden, op te stellen en toe te voegen. In het ontwerp dient een beschrijving gegeven te worden voor: • OSI laag-2 functionaliteiten; • OSI laag-3 functionaliteiten; • routing; • filtering; • voorkeur verkeersverdeling; • methode voor het kiezen van het beste pad en bij uitval; • het voldoen aan de architectuur van Diginetwerk. Antwoord V6:												
Eis 11	De Wederpartij houdt toezicht op koppelnetsbeheerders bij het fysiek aansluiten op het KPS.												
Eis 12	Bij het aansluiten van een koppelnets wordt door de Wederpartij een test rapport geleverd waaruit blijkt dat aan de Aansluitvoorwaarden KPS en architectuur van Diginetwerk is voldaan.												
V7	De Wederpartij wordt gevraagd een procedure inclusief test- en acceptatieplan te beschrijven voor het realiseren van nieuwe aansluitingen waarbij een quarantaine-periode toegepast wordt om te bepalen of een nieuwe aansluiting goed geconfigureerd is voordat de aansluiting in productie genomen wordt. Deze aansluitprocedure geldt voor zowel initieel (migratie) als voor eventuele nadere aansluitingen gedurende de looptijd. Antwoord V7:												

Ref.	Omschrijving
Eis 13	De Wederpartij moet op de door de koppelnetwerkbeheerders gewenste tijdstippen aansluiten, dus ook 's avonds of in het weekend.
Eis 14	De dienst is en blijft zodanig ingericht dat deze per productiedatum voldoet en blijft voldoen aan alle eisen zoals gesteld in de meest recente BIR, VIR en VIR-BI voor privacy gevoelige informatie voor zover van toepassing op routerings-, transport- en datacenterdiensten.
Eis 15	Op de dienst zelf en de corresponderende middelen en processen zijn en blijven per productiedatum de actuele BIR/BIO informatiebeveiligingsnormen van de overheid, gebaseerd op de ISO-27001 en 27002 van toepassing voor zover van toepassing op routerings- en transportdiensten.
Eis 16	De Wederpartij stelt twee poorten (1Gb en 10Gb) en ruimte (1U) beschikbaar aan het NCSC ten behoeve van het inbouwen van een Nationale Detectie Netwerk sensor van het NCSC op de locaties van KPS.
Eis 17	De Wederpartij stelt twee afzonderlijke spannings-groepen ter beschikking conform TIA-942 tier 3 waarop de Nationale Detectie Netwerk sensor wordt aangesloten.
Eis 18	Het KPS voorziet in de mogelijkheid om netwerkverkeer af te kunnen tappen op alle koppelvlakken, zodat dit kan worden geïnspecteerd door netwerk en/of security appliances, zonder afbreukrisico op de beschikbaarheid van het KPS.
Eis 19	Het KPS zorgt voor een netwerkkoppelvlak ten doel van managementactiviteiten voor de Nationale Detectie Netwerk sensor van de NCSC en draagt zorg van de bereikbaarheid hiervan op het KPS.

3.3. Het beheer

De Wederpartij zorgt voor de inrichting en het beheer van het KPS, regelt en contracteert de locaties en zorgt voor de toegang op de locaties voor de koppelnetwerkbeheerders. Tevens rapporteert de Wederpartij over de dienstverlening en is hij het eerste aanspreekpunt en coördinator bij incidenten en verstoringen in het berichtenverkeer tussen de koppelnetwerken.

Ref.	Omschrijving
Eis 20	De KPS dienst is 24 uur per dag, elke dag van het jaar beschikbaar.
Eis 21	De Wederpartij beschikt over een NOC (Network Operations Center) dat 24 uur per dag telefonisch en per email bereikbaar is en direct kan ingrijpen op de werking van het KPS.
Eis 22	De Wederpartij is minimaal tijdens werkdagen en kantooruren (9.00 – 17.00 uur) telefonisch en per email bereikbaar en is 7*24 telefonisch en per email bereikbaar voor incidenten.

Ref.	Omschrijving
V8	Geef aan hoe de bereikbaarheid van het NOC en beschikbaarheid van relevante expertise (bijvoorbeeld BGP) voor deze opdracht wordt gegarandeerd per type incident, incl. escalatieschema. Antwoord V8:
Eis 23	Voor de apparatuur en eventuele diensten die onderliggend zijn aan iedere KPS-locatie worden met MTBF/MTTR-getallen onderbouwde SLA's afgegeven waarmee de beschikbaarheid van de gehele KPS-voorziening op jaarbasis wordt gerealiseerd.
V9	De Wederpartij wordt gevraagd een concept SLA op te stellen voor deze opdracht. Dit concept SLA dient als basis voor de uiteindelijke contractuele SLA. Het SLA gaat daarbij tenminste in op de SLA KPI's voor: • Levering van de KPS dienst; • Levering van aansluiting op de KPS dienst; • Performance van de KPS dienst; • Wijziging op de KPS dienst; • Incidentopheffing van de KPS dienst; • Facturatie van de KPS dienst; • Rapportage over bovenstaande items. Antwoord V9:
Eis 24	De Wederpartij bewaakt continu op basis van 7 x 24 de beschikbaarheid en de werking van de dienst en alle onderliggende apparatuur en onderliggende diensten.
Eis 25	De Wederpartij maakt verkeersstatistieken van het KPS in de vorm van grafieken beschikbaar voor Logius en de koppelnets-beheerders. Hieronder worden minimaal de delay, packet-loss en belasting per poort weergegeven.
V10	Geef aan welke relevante verkeersstatistieken zullen worden gerapporteerd en lever een voorbeeldgrafiek aan van de verkeersstatistieken en de beschikbaarheid van de dienst en onderliggende apparatuur. Antwoord V10:
Eis 26	Beheer op afstand vindt out-of-band plaats. Hierbij wordt bedoeld dat het beheerverkeer niet dezelfde verbindingen gebruikt als het dataverkeer van het KPS.
V11	De Wederpartij wordt gevraagd uit te werken hoe hij het beheer op afstand realiseert, inclusief de motivering van te maken afwegingen voor het beheer op afstand. Antwoord V11:

Ref.	Omschrijving
Eis 27	Beheerverkeer wordt versleuteld tussen de eindpunten met een sleutellengte van minstens 256 bits. De gebruikte sleutellengten, cryptografische schema's en algoritmen dienen op het moment van gebruik door NIST (NIST SP800-131A, actuele versie) als veilig en toekomstbestendig te zijn geclassificeerd. Indien de eisen vanuit NIST conflicteren met de Europese regelgeving, dan dient het ENISA rapport (ENISA Key size and parameters report, meest actuele versie) gevolgd te worden.
Eis 28	Indien beheer op afstand niet mogelijk is, dan voert de Wederpartij ter plekke alle vormen van beheer uit die nodig zijn om de dienst beschikbaar te maken, zonder afhankelijkheden van connectiviteit naar elders.
Eis 29	Onderhoud aan het KPS kan door het redundante karakter van KPS uitgevoerd worden zonder impact op beschikbaarheid en vindt alleen plaats op werkdagen tussen 22:00 uur en 0:00 uur. In geval er moet worden afgeweken van deze tijdsvensters, met in acht neming dat dit twee weken vooraf dient te worden overeengekomen met Logius, zijn werkzaamheden na 0:00 uur en/of in het weekeinde mogelijk.
Eis 30	Er vindt nooit regulier onderhoud plaats op alle KPS-locaties tegelijkertijd; per periode van 24 uur kan slechts onderhoud aan één KPS-locatie plaatsvinden.
Eis 31	Onderhoud wordt zo gepland dat als er tijdens het onderhoud van de ene KPS-locatie een storing plaatsvindt op een andere KPS-locatie, het onderhoud binnen 10 minuten gestopt kan worden en de KPS-locatie waar onderhoud plaatsvond weer operationeel is.
V12	De Wederpartij wordt gevraagd toe te lichten hoe hij ervoor zorgt dat er 24 uur per dag, iedere dag van het jaar, per direct een beroep kan worden gedaan op zijn medewerkers met alle relevante kennis van de technologie waaruit de dienst is opgebouwd.
	Antwoord v12:
Eis 32	De Wederpartij bewaakt de beschikbaarheid van de netwerkketen van het Diginetwerk (AO-koppelnets-KPS-koppelnets-AO) met de door Logius beschikbaar gestelde centrale monitoring voorziening. De Wederpartij heeft een inspanningsverplichting om bij vermoeden van incidenten buiten het KPS de betreffende koppelnetsbeheerder aan te spreken op het verhelpen van netwerkstoringen conform Diginetwerk DAP en de melding en afmelding in haar eigen ticketing systeem te registreren zodat Wederpartij over doorlooptijden kan rapporteren aan Logius. De Wederpartij voert de regie vanaf het moment van het melden van een incident in de gehele keten aan Wederpartij tot en met het moment dat het incident is verholpen. Hierbij is het niet van belang of het incident binnen KPS optreedt of daarbuiten.
Eis 33	Alles wat als informatiebeveiligingsincident kan worden opgevat, zoals beschreven in hoofdstuk 16 van de BIR2017, wordt direct aan Logius gemeld.

Ref.	Omschrijving
Eis 34	Jaarlijks vindt er een uitwijktest plaats. De uitwijktest vindt plaats tussen 0:00 en 4:00 uur. Tijdens de uitwijktest worden uitvalscenario's gesimuleerd. De testscenario's worden door Logius in overleg met de koppelnetsbeheerders en de Wederpartij opgesteld. De Wederpartij werkt mee aan het voorbereiden, uitvoeren en evalueren van de test.
Eis 35	Jaarlijks verstrekt de Wederpartij Logius een TPM verklaring over de kwaliteit van de dienstverlening en de informatiebeveiliging, conform de eisen Eis 1, Eis 14 en Eis 15 in het 1e kwartaal van het jaar. De voorkeur gaat hierbij uit naar een SOC 2 type 2 audit of een ISAE3402 type 2 audit, waarbij aanvullend specifiek wordt ingegaan op de naleving van de uitvoeringsverordening EU 2018/151.
Eis 36	Na het in productie gaan van de KPS dienst levert de Wederpartij Logius een TPM verklaring waaruit conformiteit blijkt aan alle eisen gesteld in deze specificatie van de Prestatie KPS en in het bijzonder aan de eisen Eis 1, Eis 14 en Eis 15, dit ter beoordeling door Logius.
V13	De Wederpartij wordt gevraagd toe te lichten hoe hij invulling geeft aan Eis 14, Eis 15, Eis 35 en Eis 36 aan de hand van een voorbeeld TPM verklaring. Elementen die hierbij een rol spelen zijn o.a. (maar niet uitputtend): • Fysieke beveiliging van het datacenter; • Security awareness van het eigen en ingehuurd personeel; • VOG verklaring van het eigen en ingehuurd personeel; • Functiescheiding; • Beveiliging toegang voor beheer; • Beheersing van bevoegdheden en strenge beheersing van accounts/toegang met sterke bevoegdheden; • Logging beheerdershandelingen; • Gebruik van cryptografie; • Hardening van systemen; • Onderhoud van software/firmware; • Security en beheer processen. Antwoord V13:
Eis 37	De Wederpartij hanteert een geheimhoudingsplicht voor zijn medewerkers en eventueel door hem ingeschakelde medewerkers van onderaannemers in het kader van de uitvoering van deze opdracht.
Eis 38	Logius heeft het recht om, indien het daartoe aanleiding ziet, een audit te doen uitvoeren door een onafhankelijke auditor. De kosten hiervan zullen worden gedragen door Logius, tenzij hieruit ernstige tekortkomingen in de dienstverlening of beveiliging hiervan naar voren komen.

3.4. De locatie

De Wederpartij regelt en contracteert de locaties en zorgt voor de toegang op de locaties voor de koppelnetsbeheerders.

Ref.	Omschrijving
Eis 39	Het KPS wordt geleverd in een redundante opzet waarbij de fysieke apparatuur op minimaal twee geografisch gescheiden locaties in Nederland is geplaatst, waarbij het risico wordt voorkomen dat alle locaties tegelijk uitvallen vanwege bijvoorbeeld een vliegtuigcrash, overstroming, elektriciteitsuitval of aardbeving.
V14	Geef aan op welke adreslocaties de KPS dienst geleverd wordt. De Wederpartij geeft aan welke glasvezelkabels van de leveranciers KPN, Tele2, Eurofiber, Relined, VofafoneZiggo, NL-IX reeds binnen zijn op de voorgestelde locaties.
	Antwoord V14:
V15	Wederpartij werkt mee aan het onderbrengen van de dienstverlening in een ODC indien opdrachtgever hiertoe een gemotiveerd besluit neemt. Dit kan betekenen dat de dienstverlening wordt afgeschaald.
	Antwoord V15:
Eis 40	De fysieke locaties mogen niet in gebieden zijn gelegen die kunnen onderlopen (bv. uiterwaarden of buitendijks gebied).
Eis 41	De locaties hebben geen gedeelde afhankelijkheden, zoals stroomtoevoer, toegangssystemen, bewakingssystemen. Indien gelegen in poldergebieden, moeten de locaties in verschillende polders met gescheiden bemaling liggen.
Eis 42	Wanneer een datacenterlocatie gesloten wordt na de initiële looptijd, dan moet dit een jaar van tevoren aan Logius worden aangekondigd.
Eis 43	De kasten waarin zich apparatuur van de koppelnets bevindt, zijn alleen toegankelijk voor koppelnetsbeheerders en hun leveranciers of door hen ingeschakelde auditoren.
Eis 44	De kast waarin zich apparatuur van het KPS bevindt, is alleen toegankelijk voor de KPS-beheerder.
Eis 45	De datacenters zijn Tia942-Tier3 uitgevoerd.

3.5. Duurzaamheid

De overheid hecht grote belangen aan duurzaamheid. In de beoordeling worden de maatregelen die Wederpartij genomen heeft om de dienst duurzaam te leveren meegeteld.

Ref.	Omschrijving
Eis 46	De locaties hebben een power usage effectiveness (PUE) van maximaal 1.2, of een Datacenter infrastructure Efficiency (DCiE) van minimaal 83%.
V16	De Wederpartij wordt gevraagd om met documentatie te onderbouwen dat de datacenters die worden aangewend voor de uitvoering van de opdracht een power usage effectiveness (PUE) heeft van maximaal 1.2 of een DCiE (Datacenter infrastructure Efficiency) van minimaal 83%.
	Antwoord V16:
Eis 47	UPS-apparatuur in de locatie voldoet aan de meest recente versie van de Energy Star-normen voor energieprestaties. Zie hiervoor www.eu-energystar.org
V17	De Wederpartij wordt gevraagd aan te geven welke maatregelen getroffen zijn om de dienst duurzaam te exploiteren. Betrek in de uitwerking de 'best practices' voor energie-efficiëntie. https://ec.europa.eu/jrc/en/publication/2018-best-practice-guidelines-eu-code-conduct-data-centre-energy-efficiency-version-910 .
	Antwoord V17:

3.6. De migratie

De Wederpartij zorgt voor de migratie van het huidige naar de nieuwe KPS. Gedurende het project wordt er een expertiseteam gevormd, met deelnemers van de koppelnetswerken, die de migratie van de koppelnetswerken begeleiden. De Wederpartij dient een initieel migratieplan te overleggen die door deze groep gereviewd wordt.

De transitieperiode duurt van september tot eind december 2019. Verwacht wordt dat elke koppelnetswerkbeheerder zelf bepaalt wanneer hij wil worden gemigreerd. De Wederpartij dient een koppeling te maken tussen de bestaande en de nieuwe KPS, zodat een geleidelijke overgang mogelijk gemaakt wordt. Logius gaat er vanuit dat het opbouwen van het nieuwe KPS inclusief het inregelen van beheerprocedures en het voorbereiding TPM door de Wederpartij parallel worden uitgevoerd aan de migratie voorbereiding door de koppelnetswerkbeheerders om de transitieperiode zo beperkt mogelijk te houden.

De bestaande KPS-apparatuur is afgeschreven en zal aan het eind van de transitieperiode in overleg met de Wederpartij worden verwijderd.

De koppelnetswerkbeheerders kunnen besluiten om hun huidige apparatuur te handhaven of nieuwe apparatuur te plaatsen.

Ref.	Omschrijving
Eis 48	De Wederpartij voert de regie over de migratie en levert daartoe een migratieplan inclusief implementatie van IPv6 op KPS.
V18	De Wederpartij levert een migratieplan bij de inschrijving. In dit plan is rekening gehouden met de rol en inzet van Logius, van de koppelnetsbeheerders en van de Wederpartij en de op te leveren TPM- verklaring conform Eis 35 na de eerste migratie van een koppelnets binnen 2 maanden na ingangsdatum overeenkomst. NB: De migratie zoals beschreven dient te worden in het migratieplan, omvat de totale migratie van de huidige KPS dienst. Antwoord V18:
Eis 49	Tijdens de transitieperiode mag de bestaande dienst KPS niet verstoord worden. De Wederpartij zorgt ervoor dat er communicatie plaats kan vinden tussen het bestaande en nieuwe KPS en dat de continuïteit geborgd is.
V19	De Wederpartij wordt gevraagd een ontwerp aan te leveren van de koppeling tussen het huidige KPS en de nieuwe KPS, met daarin aangegeven hoe een migratie van een koppelnets plaats kan vinden en de continuïteit geborgd is. Antwoord V19:
Eis 50	Bij het aflopen van de overeenkomst verleent de Wederpartij volledige medewerking aan de migratie naar de opvolger van de diensten tegen marktconforme tarieven.

3.7. Innovatie

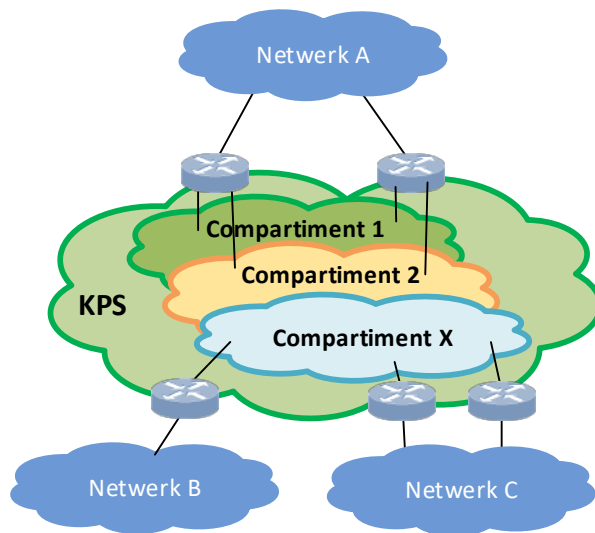
Logius zoekt een leverancier die (mede) vorm kan geven aan innovatie en doorontwikkeling van het KPS. Ofschoon vooraf niet is te voorspellen welke innovaties gewenst zijn, geven we hieronder een drietal innovaties, in verschillende stadia van ontwikkeling, waaraan op dit moment wordt gedacht. Van de Wederpartij vragen we deze innovaties te becommentariëren en te beschrijven hoe hij deze of andere innovaties samen met Logius kan vormgeven.

Extra KPS-compartmenten

Er wordt gedacht aan het realiseren van additionele (VPN) compartimenten in het KPS. Zo kunnen we ons voorstellen dat er compartimenten voor vertrouwd verkeer, onvertrouwd of Internet verkeer gewenst zijn.

Deze compartimenten dienen logisch volledig van elkaar gescheiden te zijn, verkeer van het ene naar het andere compartiment loopt uitsluitend via beveiligde koppelvlakken (de beveiligde koppelvlakken zijn geen onderdeel van deze aanbesteding). De organisaties die hun netwerk op deze compartimenten aansluiten kunnen de koppelnetsbeheerders (en dus koppelnetswerken) zijn, of andere organisaties met netwerken die kunnen

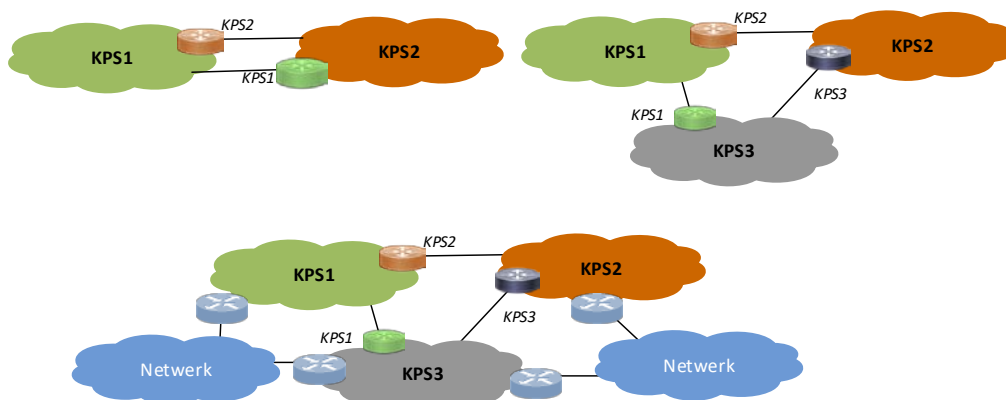
worden aangesloten. De aansluitvoorwaarden kunnen per compartiment verschillen. Indien een organisatie op meer compartimenten wil aansluiten, moet dit mogelijk zijn via een enkele fysieke interface, waarin de compartimenten door middel van VLAN's gescheiden zijn, of verschillende fysieke interfaces. De routers die op het KPS en compartimenten aangesloten worden, worden beheerd door de organisaties die op het KPS aansluiten.



figuur 5: KPS-Compartimenten

Extra KPS-leveranciers

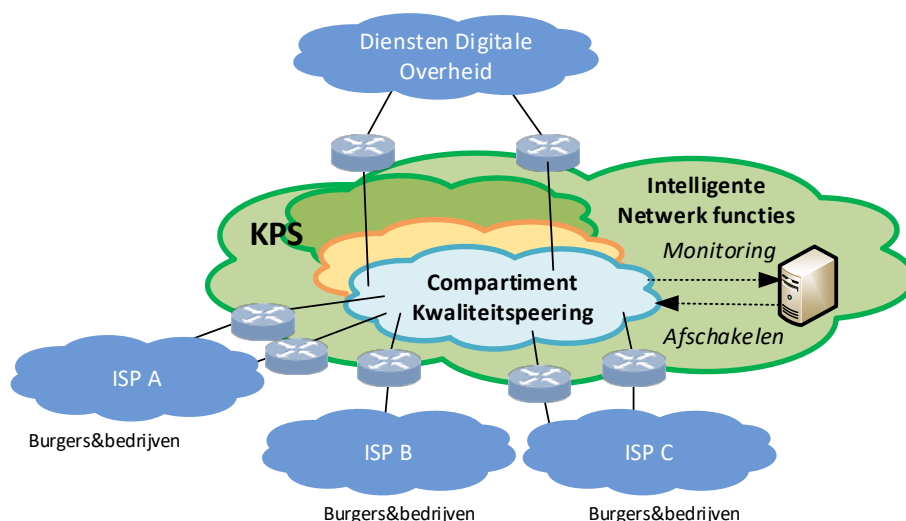
Als knooppunt tussen diverse overheidsnetwerken is het KPS een bouwsteen waaraan zeer hoge beschikbaarheidseisen gesteld kunnen worden. Het KPS wordt tot de vitale infrastructuur van de Overheid gerekend. Het realiseren van additionele KPS'en geleverd door één of meer andere leveranciers en op één of meer andere locaties, kan onderdeel zijn van de strategie om een zeer hoge beschikbaarheid te realiseren. De KPS'en dienen aan elkaar gekoppeld te worden waarbij tussen deze KPS'en op basis van BGP zal worden gerouteerd. Elke leverancier realiseert één verbinding naar de andere KPS'en en zorgt dat verkeer gerouteerd wordt. De (koppel)netwerken kunnen op een selectie van KPS'en aansluiten en zo redundantie realiseren.



figuur 6: KPS leveranciers

Kwaliteitspeering

Eén van de hiervoor genoemde extra compartimenten zou bijvoorbeeld gebruikt kunnen worden als koppelpunt (peeringpoint) waar de overheid digitale diensten aanbiedt aan burgers en bedrijven. Door hier directe koppelingen te realiseren met de (grote) ISP's in Nederland ontstaat een directere en betrouwbaarder internetverbinding tussen de digitale diensten en de gebruikers. Om onbeschikbaarheid door DDOS-aanvallen te voorkomen is monitoring van het verkeer gewenst, waarbij een peer automatisch afgeschakeld wordt als er veel niet-legitiem verkeer over de verbinding binnen komt. Een soortgelijk peeringconcept zou ook voor verschillende cloudproviders gebruikt kunnen worden, waarbij verschillende overheidsorganisaties gebruik maken van één of enkele centrale koppelingen met cloudproviders.



figuur 7: Kwaliteitspeering

Ref.	Omschrijving
Eis 51	Het dient mogelijk te zijn om cloudproviders aan te laten haken aan het KPS.
V20	Licht toe aan de hand van een beschrijving hoe de participatie van cloudproviders bij het KPS kan worden gerealiseerd met in achtneming van de Aansluitvoorwaarden KPS en de architectuur van Diginetwerk. Antwoord: V20:
Eis 52	Ook bij doorontwikkeling dienen de open (verplichte) standaarden te worden toegepast (pas-toe-of-leg-uit-principe) (https://www.forumstandaardisatie.nl/open-standaarden).
Eis 53	De Wederpartij dient een extra KPS-compartiment, logisch gescheiden van het eerder gevraagde knooppunt te kunnen toevoegen aan de dienstverlening.

Ref.	Omschrijving
V21	De Wederpartij wordt gevraagd aan te geven hoe hij extra KPS-compartimenten kan bieden in de dienst en welke risico's hierbij worden onderkend en gemitigeerd in relatie tot de aansluitvoorwaarden KPS en de architectuur van Diginetwerk.
	Antwoord V21:
Eis 54	De Wederpartij dient samen met (een) eventuele andere KPS-leverancier de KPS dienst te kunnen bieden, waarbij een afbakening van de dienst per leverancier plaats gaat vinden.
V22	De Wederpartij wordt gevraagd aan te geven hoe hij met (een) eventuele andere KPS-leveranciers de dienst kan leveren en welke randvoorwaarden gesteld dienen te worden.
	Antwoord V22:
V23	De Wederpartij wordt gevraagd aan te geven hoe hij kwaliteitspeering kan implementeren in de dienst en welke risico's daarbij worden onderkend en gemitigeerd.
	Antwoord V23:
V24	De Wederpartij wordt gevraagd welke innovaties hij kan voorstellen om de dienst nog beter te laten aansluiten op de behoefte van nu en in de toekomst.
	NB: De kosten die hiermee samenhangen zullen uit het innovatiebudget worden gefinancierd.

Begrippen en afkortingen

Begrip / Afkorting	Toelichting
AED	A anbieder van E ssentiële D iensten
Afnemer	Een overheidsorganisatie die gebruik maakt van een aansluiting op Diginetwerk.
AIVD	A lgemene I nlichtingen en V eiligheids D ienst
AO	A angesloten O rganisatie, een overheidsorganisatie die gebruik maakt van een aansluiting op Diginetwerk.
ARP	A ddress R esolution P rotocol
AS-nummer	A utonomous S ystem-nummer
BDPU	B ridge P rotocol D ata U nit
Beschikbaarheid (norm)	De mate waarin de dienst in bedrijf is op het moment dat een organisatie deze nodig heeft. Betreffende de infrastructuur: De mate waarin een dienst bruikbaar is op het moment dat hier behoefte aan bestaat.
Beveiliging	Het pakket van maatregelen ter waarborging van de beschikbaarheid, integriteit en exclusiviteit van de informatie welke via Diginetwerk wordt verstuurd of ontvangen door de afnemer.
Beveiligings-incident	Een situatie waarbij de beschikbaarheid, integriteit en of de exclusiviteit van de dienst niet meer volgens afspraak geborgd kan worden.
BGP	B order G ateway P rotocol
Bijzondere informatie	Staatsgeheimen en overige bijzondere informatie waarvan kennisname door niet gerechtigden, nadelige gevolgen kan hebben voor de belangen van de staat, haar bondgenoten of een of meer ministeries.
BIO	B aseline I nformatiebeveiliging O verheid
BIR	B aseline I nformatiebeveiliging R ijksdienst
BKWI	B ureau K etenbeheer W erk en I nkomen, organisatieonderdeel van het UWV
Calamiteit	Een ongeplande situatie waarbij verwacht wordt dat de duur van het niet beschikbaar zijn van een of meer diensten, de afgesproken drempelwaarde zal overschrijden.
CUG	C losed U ser G roups
DAP	D ossier A fspraken en P rocedures
Datacenter	De huisvesting van een deel van de KPS dienst en aansluitkoppelvlakken.
DCiE	D ata C enter infrastructure E fficiency
DDoS	D istributed D enial of S ervice
Dep.V	Bijzondere informatie welke niet als staatsgeheim wordt aangemerkt, wordt gerubriceerd als Departementaal Vertrouwelijk (Dep.V) indien kennisname hiervan door niet gerechtigden, nadeel kan toebrengen aan het belang van een of meer ministeries.
Diginetwerk	Afsprakenstelsel voor het koppelen van besloten netwerken van de overheid
DNS	D omain N ame S ystem
Eis	Fundamentele eis voor de dienst. De benoemde functionaliteit moet in het eindresultaat terugkomen. Het niet voldoen aan deze eis wordt als een ernstige tekortkoming gezien.

Begrip / Afkorting	Toelichting
Encryptie	Een proces waarmee gegevens met behulp van een wiskundig algoritme en een cryptografische sleutel worden versleuteld, zodat deze onleesbaar zijn voor onbevoegden. De betrouwbaarheid van de encryptie hangt af van de grootte van de cryptografische sleutel, het gebruikte algoritme, de implementatie ervan evenals de gebruikersdiscipline.
EU	E uropese U nie
Exclusiviteit	De mate waarin de toegang tot en de kennisname van een informatiesysteem en de informatie daarin is beperkt tot een gedefinieerde groep gerechtigden.
HTTP	H yper T ext T ransfer P rotocol Protocol voor de communicatie tussen een webclient en een webserver.
HTTPS	H yper T ext T ransfer P rotocol S ecure Als bij HTTP maar de communicatie wordt hierbij versleuteld.
ICMP	I nternet C ontrol M essage P rotocol Netwerkprotocol dat de administratie van een netwerk verzorgt.
Incident	Afwijking op de reguliere dienstverlening, zoals gedefinieerd volgens ITIL.
Integriteit	De mate waarin een systeem zonder fouten is. De zekerheid dat gegevens volledig zijn en ongewijzigd, ongeacht of dit opzettelijk, onopzettelijk door menselijk toedoen of anderszins is gebeurd.
ISO	I nternationale O rganisatie voor S taandaardisatie
ISP	I nternet S ervice P rovider
ITIL	I nformation T echnology I nfrastructure L ibrary Methodiek bestaande uit best practices voor het inrichten van ICT beheer processen
Koppeling	Verbinding tussen afnemer en Diginetwerk. Een afnemer kan meerdere koppelingen afnemen.
Koppelnets	Door een leverancier beheert netwerk dat onderdeel vormt van Diginetwerk, waarop afnemers aangesloten kunnen worden.
Koppelnets-beheerder	Leverancier die het beheer voert over het koppelnets
KPI	K ey P erformance I ndicator
KPS	K oppelnets P ublieke S ector, knooppunt van koppelnets binnen Diginetwerk.
KPS-beheerder	Leverancier die het KPS gaat beheren.
Kwaliteit	De mate waarin het geheel van eigenschappen van de dienst voldoet aan de uit het gebruiksdoel voortvloeiende eisen en wensen.
Logius	Aanbestedende dienst, onderdeel van het Ministerie van Binnenlandse zaken.
MAC	M edia A ccess C ontrol
MED	M ulti E xit D iscriminator
MLAT	M utual L egal A ssistance T reaty
MTBF	M ean T ime B etween F ailures, De gemiddelde tijd tussen- twee verstoringen van een dienst of voorziening.

Begrip / Afkorting	Toelichting
MTTR	Mean Time To Repair , De gemiddelde tijd die nodig is om de dienst te herstellen na het optreden van een verstoring.
MTU	Maximum Transmission Unit
NOC	Network Operations Center
NCSC	Nationaal Cyber Security Centrum
ODC	OverheidsDataCenter
Policy	Een set van maatregelen om een bepaald doel te bereiken.
Productiedatum	De datum waarop de dienst geleverd wordt na de eerste succesvolle migratie.
Protocol	Gedragsovereenkomst. Het wordt in dit document gebruikt om communicatie en computerprotocollen aan te duiden.
PUE	Power Usage Effectiveness
PvE	Specificatie van de Prestatie Beschrijving van de eisen en wensen waaraan een te leveren product of dienst dient te voldoen.
QoS	Quality of Service
OSI	Open Systems Interconnect
RijksDNS	DNS voorziening voor de Rijksoverheid, beschikbaar op Diginetwerk.
RIPE	Réseaux IPEuropéens , Europese RIR
RIR	Regional Internet Registry
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SOA	Statement Of Account
SOC	Service Organization Control
STP	Spanning Tree Protocol
TIA	Telecommunications Industry Association
TPM	Third Party Mededeling
UPS	Uninterruptable Power Supply
VIR	Voorschrift Informatiebeveiliging Rijksdienst
VIR-BI	Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
Wbni	Wet beveiliging netwerk en informatiesystemen
Wederpartij	Wederpartij van KPS (tenzij in de context anders is aangegeven)