



Diginetwerk Architectuurdokument

[Diginetwerk Architectuurdokument](#)

Het doel van dit dokument is het beschrijven van de overkoepelende architectuur van het Afsprakenstelsel Diginetwerk. In dit dokument worden de vragen beantwoord: 'Wat is Diginetwerk?' en 'Waaruit is het Afsprakenstelsel Diginetwerk opgebouwd?'

Versiegegevens

Publicatiedatum: 15 februari 2024

Versie: 1.6

1. Inleiding

Het doel van dit dokument is het beschrijven van de overkoepelende architectuur van Diginetwerk. In dit dokument worden de vragen beantwoord: "Wat is Diginetwerk?" en "Waaruit is het Diginetwerk opgebouwd?". Deze antwoorden helpen beleidsmedewerkers binnen de overheid en private Koppelnetaanbieders om te bepalen of een voorziening of toepassing gebruik kan maken van Diginetwerk en wat de voordelen zijn. Tevens specificeert dit dokument eisen waaraan deelnemers in het stelsel moeten voldoen en geeft hiermee richting aan ontwerpers en architecten die werkzaam zijn bij de deelnemers.

De deelnemers aan het stelsel zijn de Koppelnetaanbieders, de KPS-aanbieder en de Aangesloten Organisaties.

Scope

Dit dokument beperkt zich tot de beschrijving van de architectuur van het Diginetwerk, de technische afspraken en rollen. Het dokument beschrijft geen aansluit- en beheerprocessen, aansluitvoorwaarden en SLA's. Deze worden in andere onderdelen van de documentatieset Diginetwerk beschreven, zoals de Dienstbeschrijving, DAP en Aansluitvoorwaarden.

Status

Het voorliggend architectuurdokument wordt vastgesteld door het Tactisch Beraad Diginetwerk. De definitieve versie wordt gepubliceerd op de Logius-website. Deze versie geldt als norm voor het gehele Afsprakenstelsel Diginetwerk. De Koppelnetaanbieders, Aangesloten Organisatie en de KPS-aanbieder dienen hun aansluiting en/of koppelvlak met Diginetwerk volgens deze norm in te richten.

Samenhang met NORA

De Nederlandse Overheid Referentie Architectuur (NORA) is gerelateerd aan dit dokument. In NORA zijn de beveiligingsniveaus en de aanpalende maatregelen beschreven die het Afsprakenstelsel Diginetwerk gebruikt als uitgangsprincipes. Dit is verwoord in hoofdstuk 3 [NORA](#) beschrijft Diginetwerk als het voorkeurskanaal voor interne overheidscommunicatie

2. Introductie Diginetwerk

Dit hoofdstuk geeft een globaal overzicht van Diginetwerk en beschrijft de terminologie die in het dokument wordt gebruikt.

Begrippen Afsprakenstelsel Diginetwerk

- **Afnemer** Een publiekrechtelijke of privaatrechtelijke organisatie met een publieke taak, alsmede in geval van een overheidsorganisatie, het samenwerkingsverband waarvan de overheidsorganisatie onderdeel is, die voor de uitoefening van die publieke taak digitaal verkeer met andere organisaties wenselijk acht en dit verkeer uit oogpunt van informatiebeveiliging via een besloten digitaal communicatienetwerk wil laten plaatsvinden. Bij Partijen tevens bekend als Aangesloten Organisatie.
- **Derde** Elke partij die geen Partij is bij deze Overeenkomst. In de zin van deze Overeenkomst wordt daarmee bijvoorbeeld een dienstaanbieder aangeduid die een dienst aanbiedt via Diginetwerk aan een Afnemer of een door Partijen ingeschakelde Derde zoals een onderaannemer. Afnemer is, net als Partijen, verplicht om te toetsen of Derde voldoet aan alle eisen die gesteld zijn aan een koppeling met Diginetwerk.
- **Beveiligd Koppelvlak** Het geheel van gemeenschappelijke beveiligingsafspraken en ICT-voorzieningen die het uitwisselen van elektronische informatie tussen aangesloten ketenpartners mogelijk maakt. Deze uitwisseling is zo veel mogelijk onafhankelijk van, en pleegt geen inbreuk op, de eigen bedrijfsprocessen, bescherming van (persoons)gegevens, applicaties en infrastructuur van de betreffende ketenpartner.
- **Diginetwerk** Zowel de benaming van het Afsprakenstelsel voor het koppelen van besloten netwerken, de zogenoemde Koppelnetaanbieders aan het KPS, als ook het virtuele netwerk dat op dit Afsprakenstelsel gebaseerd is. Door onderlinge afspraken en de implementatie van de Diginetwerk Architectuur en de Diginetwerk-uitgangspunten, functioneert het als één geheel. De Aangesloten Organisaties kunnen elkaar op een veilige wijze via één aansluiting bereiken.

- **Diginetwerkaansluiting** Een Diginetwerkaansluiting is een IP-gerouteerd netwerkkoppelvlak, dat uitsluitend geleverd kan worden door een Koppelnetaanbieder die een samenwerkingsovereenkomst heeft met Logius. Kenmerk van de Diginetwerkaansluiting is dat zij wordt geleverd via de besloten infrastructuur van de Koppelnetaanbieder waardoor het transport gescheiden is van internet. Een Diginetwerkaansluiting wordt niet via internet geleverd.
- **Koppelnetaanbieder** De centrale netwerkvoorziening die datatransport tussen verschillende Koppelnetwerken faciliteert voor Diginetwerk.
- **Koppelnetaanbieder** Een besloten netwerk dat onderdeel vormt van Diginetwerk conform de gedefinieerde architectuur van Diginetwerk zoals opgenomen in het Diginetwerk Architectuurdocument.
- **Koppelnetaanbieder** De (semi) overheids- of private organisatie die middels een samenwerkingsovereenkomst met Logius aansluiting heeft verkregen op het Diginetwerk en haar infrastructurele diensten aanbiedt aan een Afnemer middels een besloten Koppelnetaanbieder waar zij eigenaar en/of beheerder van is.
- **KPS-aanbieder** De KPS-aanbieder voert regie op ontwikkeling, beheer en exploitatie van het KPS. De KPS-aanbieder stelt de KPS-dienst beschikbaar aan de Koppelnetaanbieders en is opdrachtgever aan de KPS-leverancier voor het leveren van de KPS-dienst.
- **KPS-Leverancier** De KPS-leverancier levert en beheert het Koppelnetaanbieder (KPS) in opdracht van de KPS-aanbieder.
- **Samenwerkingsovereenkomst** Met Samenwerkingsovereenkomst wordt bedoeld de getekende overeenkomst tussen Koppelnetaanbieder en Logius.
- **Samenwerkruimte Diginetwerk** Dit is de besloten omgeving waarin Logius informatie deelt met alle Koppelnetaanbieders voor de samenwerking, <https://www.samenwerkruimten.nl/teamsites/diginetwerk>
- **Stelselregisseur** De stelselregisseur voert regie op het Afsprakenstelsel Diginetwerk, in afstemming met de belanghebbenden en de beleidsopdrachtgever Ministerie BZK. De stelselregisseur beheert de stelseldocumenten; de bijlagen bij deze samenwerkingsovereenkomst, geeft advies over nieuwe ontwikkelingen en stemt af met potentiële nieuwe Koppelnetaanbieders.
- **Strategisch Beraad Diginetwerk** Overleg op strategisch beheerniveau, waarin alle Koppelnetaanbieders vertegenwoordigd zijn en eveneens deel van uitmaken.
- **Tactisch Beraad Diginetwerk** Overleg op Tactisch Beheerniveau waarin alle Koppelnetaanbieders vertegenwoordigd zijn en eveneens deel van uitmaken.
- **Operationeel Overleg** Overleg op operationeel beheerniveau, waarin alle Koppelnetaanbieders vertegenwoordigd zijn en eveneens deel van uitmaken.

Context Diginetwerk

Diginetwerk is een afsprakenstelsel voor het koppelen van besloten netwerken voor de overheid, zodat overheidsorganisaties en organisaties en hun leveranciers met een publieke taak via deze gekoppelde netwerken onderling op veilige en betrouwbare wijze gegevens kunnen uitwisselen.

Het afsprakenstelsel realiseert een besloten logisch netwerkdomein voor communicatie tussen overheidsorganisaties. Voor dit domein wordt de naam Diginetwerk gebruikt. Dit naar analogie met Internet, dat technisch een logisch netwerk is, maar ook te beschouwen is als afsprakenstelsel van netwerken van verschillende aanbieders.

Diginetwerk is daarmee echter niet een eenduidige technische netwerkvoorziening, onder beheer van één uitvoeringsorganisatie. Iedere Koppelnetaanbieder is zelf verantwoordelijk voor het beheer van zijn netwerk en de koppeling met de daarop aangesloten organisaties. Een organisatie neemt een aansluiting op Diginetwerk, door een aansluiting te nemen op een (of meerdere) Koppelnetwerken die deel uitmaken van het Afsprakenstelsel Diginetwerk.

In dit document wordt gesproken over “Afsprakenstelsel Diginetwerk” wanneer het afsprakenstelsel wordt bedoeld en over “Diginetwerk” wanneer het logisch netwerkdomein wordt bedoeld.

Doel van Afsprakenstelsel Diginetwerk

Het doel van het Afsprakenstelsel Diginetwerk is een veilige, efficiënte en effectieve standaardoplossing te bieden voor elektronische gegevensuitwisseling tussen overheidsorganisaties en 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 netwerken en zonder afhankelijkheid van internet.

Diginetwerk biedt veilige en betrouwbare netwerkverbindingen via een besloten infrastructuur, in tegenstelling tot publieke verbindingen over internet. Hierdoor kunnen meer garanties ten aanzien van veiligheid en betrouwbaarheid geboden worden. Diginetwerk biedt met name voordelen met betrekking tot de end-to-end beschikbaarheid van informatie-uitwisseling tussen aangesloten organisaties.

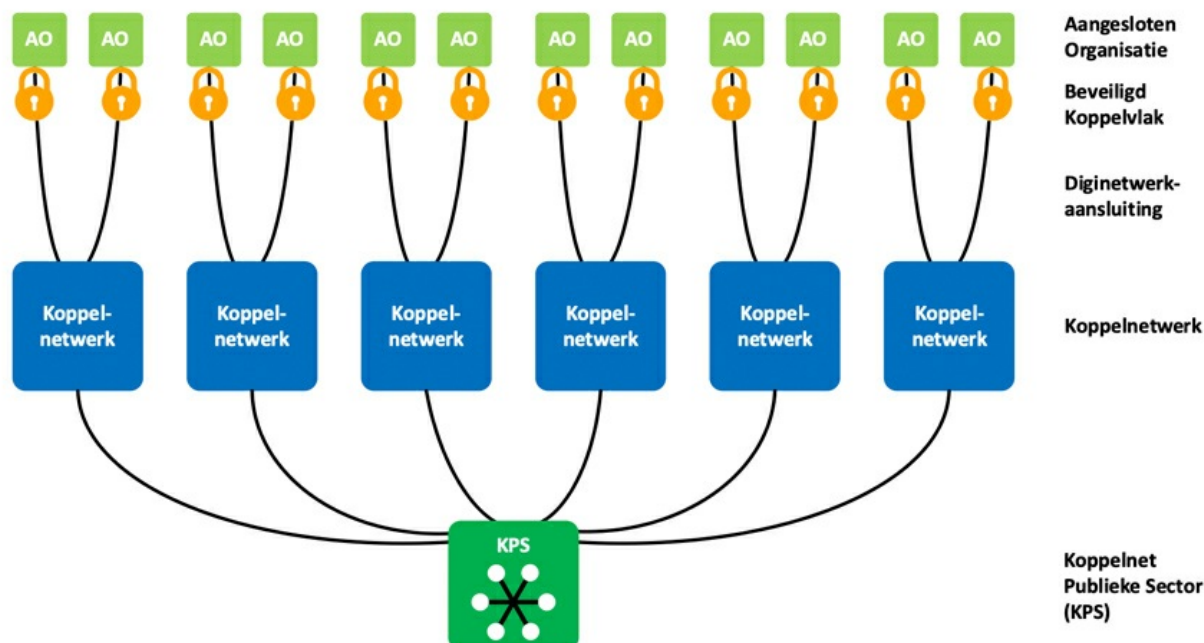
Netwerk van netwerken

Het Diginetwerk is ontstaan door het koppelen van een aantal besloten netwerken van de Overheid, waardoor het niet meer noodzakelijk was om voor iedere onderlinge koppeling een separate netwerkverbinding aan te leggen. Hierdoor konden kosten worden bespaard. In de loop der jaren zijn meerdere overheidsnetwerken aan Diginetwerk toegevoegd en is het gebruik sterk toegenomen. Anno 2021 is Diginetwerk het grootste netwerk voor communicatie tussen de verschillende overheidsorganisaties en organisaties met een publieke taak.

De aan het Afsprakenstelsel Diginetwerk deelnemende en autonoom beheerde netwerken worden **Koppelnetwerken** genoemd. Een organisatie die een aansluiting op een van de Koppelnetwerken heeft, heet een **Aangesloten Organisatie**. Het knooppunt waar alle Koppelnetwerken onderling verbonden zijn heet het **Koppelnetaanbieder (KPS)**. Het geheel aan Koppelnetwerken en het KPS vormt het Diginetwerk.

Door gemeenschappelijk afspraken te maken op het gebied van connectiviteit, beschikbaarheid, beveiliging en het gebruik van standaarden kan iedere Aangesloten Organisatie via Diginetwerk communiceren met andere organisaties, met slechts één aansluiting op een van de Koppelnetwerken. Het Afsprakenstelsel Diginetwerk is gebaseerd op gemeenschappelijk aansluitvoorwaarden, beheerafspraken, de dienstbeschrijving en dit architectuurdocument.

Het concept van Afsprakenstelsel Diginetwerk wordt in figuur 1 weergegeven:



Figuur 1: Concept Afsprakenstelsel Diginetwerk

Voordelen Koppelnets

Voor de Koppelnetsaanbieder heeft Afsprakenstelsel Diginetwerk de volgende voordelen:

- Het vormt één groot overheidsnetwerkdomein waar in potentie alle meer dan 1600 Nederlandse overheidsorganisaties [] en hun leveranciers een aansluiting op hebben.
- Overheidsorganisaties en hun leveranciers hebben keuzevrijheid bij welke Koppelnetsaanbieder zij een Diginetwerkaansluiting afnemen.
- De Koppelnetsen zijn via het centrale Koppelnets Publieke Sector (KPS) met elkaar verbonden. Een Koppelnetsaanbieder maakt op eenvoudige wijze een redundante aansluiting op het KPS om daarmee verbonden te zijn met de gehele overheid.
- Het afsprakenstelsel heeft eenduidige architectuur- en serviceafspraken waarmee interoperabiliteit tussen de verschillende Koppelnetsen mogelijk wordt gemaakt.

Voordelen voor de Aangesloten Organisatie

Voor de Aangesloten Organisatie heeft Afsprakenstelsel Diginetwerk de volgende voordelen:

- Het besloten karakter van het Diginetwerk zorgt voor een veiliger alternatief dan het internet voor het uitwisselen van gegevens tussen overheidsorganisaties. Diginetwerk biedt met name voordelen met betrekking tot de end-to-end beschikbaarheid van informatie-uitwisseling tussen aangesloten organisaties.
- Met één netwerkaansluiting kan efficiënt en betrouwbaar gecommuniceerd worden met alle aangesloten overheidsorganisaties en hun leveranciers
- Beschikbaarheid van de connectiviteit wordt geborgd door een Service Level Agreement (SLA) over de gehele keten
- Er is keuzevrijheid voor publieke of private Koppelnetsaanbieders
- Er is keuzevrijheid voor een aansluiting op een of meerdere Koppelnetsen
- Het zorgt voor het op een eenduidige wijze diensten aanbieden en/of afnemen via Diginetwerk met andere aangesloten organisaties. Zo bereiken organisaties een betere kwaliteit tegen lagere kosten

Governance

De governance van Diginetwerk is beschreven in het document "Governance Diginetwerk".

Betrokken Koppelnetsen

De Koppelnetsaanbieders die een Diginetwerkaansluiting leveren staan beschreven op de [Logius-website](#).

Organisaties die een besloten datanetwerk exploiteren en willen toetreden tot het Afsprakenstelsel Diginetwerk als Koppelnetsaanbieder, kunnen contact opnemen met Logius voor informatie over [de toetredingseisen en het toetredingsproces](#).

3. Principes, uitgangspunten en ontwerpbeslissingen

Kader

De essentie van het gebruikte concept voor Diginetwerk is:

- Afsprakenstelsel van besloten netwerken
- Onafhankelijk van internet voor datatransport (besloten netwerk)

- Zoveel mogelijk hergebruik van bestaande besloten overheidsnetwerken
- Interoperabiliteit door toepassen van bewezen internetstandaarden

Het uitgangspunt voor Diginetwerk is het hergebruik van bestaande en bewezen internetstandaarden om besloten interoperabiliteit te realiseren in een afspraken stelsel. Het voorbeeld is internet, dit is immers al een bewezen afsprakenstelsel van gekoppelde netwerken met interoperabiliteit op wereldschaal.

Generieke Principes

NORA is gebruikt als kader voor de generieke principes van Afsprakenstelsel Diginetwerk. De volgende afgeleide principes van NORA zijn als uitgangspunten voor Afsprakenstelsel Diginetwerk van toepassing:

- AP01** Diensten zijn herbruikbaar. Diginetwerk bestaat uit herbruikbare diensten (koppelnetswerken, Rijks-DNS, etc.). Aangeboden diensten binnen Diginetwerk zijn zodanig opgezet dat andere organisaties deze kunnen hergebruiken.
- AP05** De dienst is nauwkeurig beschreven.
- AP06** De dienst maakt gebruik van standaard oplossingen.
- AP07** De dienst gebruikt open standaarden volgens de pas-toe-of-leg-uit lijst.
- AP021** De dienst wordt gebundeld met verwante diensten.
- AP025** Transparante dienstverlening.
- AP028** Afspraken zijn vastgelegd.

*De nummering van NORA is overgenomen

Ontwerpprincipes

Aanvullend op de generieke principes gelden de volgende ontwerpprincipes voor Afsprakenstelsel Diginetwerk opgesteld:

- Het netwerk kent een besloten karakter. Dat wil zeggen Diginetwerk is alleen voor partijen die voldoen aan de definitie Afnemer in de Aansluitvoorwaarden Diginetwerk. Partijen zijn gehouden aan beveiligingsmaatregelen die borgen dat hun Diginetwerkaansluiting gescheiden is van het Internet.
- OP1** Het gebruik van VPN's op basis van (encrypted) tunnels over Internet voor het leveren van een Diginetwerkaansluiting is niet toegestaan.
- OP2** Er wordt gebruik gemaakt van een uniek publiek IP-nummerplan voor Diginetwerk. Voor zowel IPv4 als IPv6 worden publieke IP-adresblokken gebruikt, die niet op internet gerouteerd worden.
- Tussen het KPS en de Koppelnetswerken wordt dynamische routing op basis van het BGP-4 protocol gebruikt. Er wordt gebruik gemaakt van publieke BGP AS-nummers die uitgegeven zijn door het RIPE NCC. Indien dit voor aanbieders niet mogelijk is, kan gebruikt gemaakt van een reeks private AS-nummers die door Logius worden uitgegeven en geregistreerd.
- OP4** Asymmetrische routing tussen het KPS en de Koppelnetswerken is toegestaan.
- OP5** Koppelnetswerken mogen onderling alleen via KPS communiceren. Directe koppelingen tussen Koppelnetswerken zijn niet toegestaan.
- OP6** De Aangesloten Organisaties resoluten diginetwerk.net, diginetwerk.nl en overheid-i.nl via een conditional forward naar de Rijks-DNS.
- OP7**

4. Vereisten

In dit hoofdstuk worden de eisen beschreven die gesteld worden aan Afsprakenstelsel Diginetwerk. Deze eisen zijn afgeleid van de algemene en ontwerpprincipes en gelden voor de Koppelnetswerken, KPS en de Aangesloten Organisaties die gezamenlijk het Afsprakenstelsel Diginetwerk vormen.

Functioneel

Diginetwerk is een schaalbaar, breedbandig en hoog beschikbaar transportnetwerk dat ondersteunend is aan de primaire taken van de overheid. Onder meer worden hieronder de volgende functies en diensten onderkend:

- Raadplegen van (basis)registers.
- Uitwisselen van gestructureerde gegevens zoals elektronische (berichten)diensten.
- Uitwisselen van ongestructureerde gegevens zoals email.
- Ontsluiten van intranet-websites.
- Gemeenschappelijk gebruik van authenticatie-diensten, sites en bestanden.
- Koppeling naar Cloud-providers.
- Datacenter-replicatie
- Datacenter-synchronisatie

Eis 1 Diginetwerk is ondersteunend aan de primaire taken van de overheid.

De belangrijkste functionele eis voor het Afsprakenstel Diginetwerk is dat de gezamenlijke besloten Koppelnetswerken één besloten logisch netwerk voor de overheid moet vormen. Er mogen geen directe koppelingen van Koppelnetswerken van Diginetwerk met openbare netwerken gemaakt worden. Datatransport via Diginetwerk moet onafhankelijk van internet kunnen werken. Voor het tot stand komen van datatransport wordt vaak gebruik gemaakt van PKI-certificaten, en eventueel andere voorzieningen die wel afhankelijk zijn van Internet. Voor dit doel is het toegestaan om een beveiligde koppeling met internet te gebruiken.

Eis 2 Datatransport via Diginetwerk is onafhankelijk van het internet. Voor PKI-certificaten en andere voorzieningen die afhankelijk zijn van internet is het toegestaan om een beveiligde koppeling met internet te gebruiken.

IP-adressen

Diginetwerk maakt gebruik van een uniek IP-nummerplan met “public” IPv4- en IPv6-adressen die niet op internet worden gerouteerd (ontwerpprincipie OP3). De overkoepelende IP-reeksen die voor dit nummerplan zijn vastgesteld worden gepubliceerd op de Samenwerkruimte Diginetwerk.

IPv4 is bij publicatie van deze versie van het Architectuurdokument het standaard protocol voor IP-adressen op Diginetwerk. De hoeveelheid vrije publieke IP-adressen in de Diginetwerk-pool is echter beperkt en kan door de wereldwijde schaarste aan publieke IPv4-adressen moeilijk aangevuld worden. Om deze reden is het noodzakelijk ook IPv6 voor Diginetwerk mogelijk te maken en is het KPS daar in 2020 geschikt voor gemaakt. In 2024 is beoogd dat alle Koppelnetswerken geschikt zijn voor IPv6.

Er is een verschil in de wijze van toekennen van IP-adressen aan Koppelnetswerken en Aangesloten Organisaties tussen IPv4 en IPv6. De oorzaak hiervan is dat voor IPv4 een historische afspraak geldt dat alleen publieke IP-adressen uit door Logius beheerde IP-reeksen worden toegekend, terwijl bij IPv6 de afspraken uit het Overheidsbreed IPv6-nummerplankader gelden, waarbij een organisatie een serie IPv6-reeksen krijgt voor gebruik op Internet, Diginetwerk en andere besloten Overheidsnetswerken.

IPv4

Voor IPv4 is het uitgangspunt dat een Aangesloten Organisatie een IP-reeks voor Diginetwerk ontvangt van zijn Koppelnetswerkenaanbieder. Een IPv4-adres op Diginetwerk is daarmee standaard Koppelnetswerkenafhankelijk (*vergelijkbaar met Provider-aggregatable address space (PA) op internet*).

Logius beheert een aantal grote blokken publieke IPv4-adressen. Logius geeft hieruit grote IP-reeksen uit aan de Koppelnetswerkenaanbieders, die ze verder verdelen onder de Aangesloten Organisaties.

Voor Koppelnetswerken KPN AoD geldt een historische uitzondering dat zij zelf een aantal blokken publieke IPv4-adressen uit haar eigen voorraad op Diginetwerk gebruiken. Deze reeksen zijn opgenomen in het Diginetwerk IP-nummerplan.

Voor Aangesloten Organisaties die “multihomed” aansluiten op meerdere Koppelnetswerken zijn IP-adressen uitgegeven door een Koppelnetswerken onwerkbaar. Voor dit specifieke doel is een reeks Koppelnetswerkenonafhankelijke IPv4-adressen opgenomen in het Diginetwerk-nummerplan. Deze IPv4-adressen worden direct door Logius uitgedeeld.

Eis 3 Voor IPv4 krijgen Aangesloten Organisaties een reeks IPv4-adressen van de Koppelnetswerkenaanbieder. Voor Aangesloten Organisaties met een redundante koppeling met twee Koppelnetswerken wordt een Koppelnetswerkenonafhankelijke reeks door Logius toegekend.

IPv6

Voor IPv6 is het uitgangspunt dat een Aangesloten Organisatie zijn IP-reeks aanvraagt bij Logius. Een IPv6-adres op Diginetwerk is daarmee standaard Koppelnetswerkenonafhankelijk (*vergelijkbaar met provider-independent address space (PI) op internet*).

Deze IPv6-reeks voor Diginetwerk is onderdeel van een serie IPv6-reeksen die een organisatie krijgt toegewezen voor gebruik op netswerken met verschillende vertrouwensniveaus conform NORA. De toegekende specifieke reeksen kunnen vervolgens worden gebruikt op Internet, Diginetwerk en andere besloten Overheidsnetswerken.

Het verschil tussen de verschillende IPv6-reeksen blijkt uit het 9e hexadecimale cijfer in het IPv6-adres. Voor Diginetwerk is dit getal altijd 2. De drie daaropvolgende hex-cijfers zijn specifiek voor de organisatie die er gebruik van maakt en die op deze wijze herleidbaar is aan het IPv6-adres. Uitzondering hierop zijn een paar grote uitvoeringsorganisaties van het Rijk, die een grotere IPv6-reeks hebben ontvangen en herkenbaar zijn aan het 8e hexadecimale getal in het adres.

Voorbeeld gemeente Juinen:

Toekenning prefix Juinen	Netwerkcategorie
2A07:3500:1FF0::/46	Onvertrouwd (gebruik o.a. op Internet)
2A07:3500:2FF0::/46	Semi-vertrouwd (Diginetwerk)
2A07:3500:3FF0::/46	Semi-vertrouwd
2A07:3500:5FF0::/46	Vertrouwd

Juinen vraagt IPv6-adressen aan bij Logius en krijgt vier IPv6-reeksen toegekend. Juinen is herkenbaar aan de hexadecimale getallen FF0. Voor Diginetwerk gebruikt Juinen alleen de reeks 2A07:3500:2FF0::/46

Aangesloten Organisaties (overheden en leveranciers) vragen hun IPv6-adressen direct aan bij Logius conform de richtlijnen uit het Overheidsbreed IPv6-nummerplankader. Koppelnetswerkenaanbieders krijgen van Logius een eigen IPv6-reeks voor Koppelnetswerkenspecifieke koppelingen en diensten. Deze IPv6-adressen mogen niet gebruikt worden voor Aangesloten Organisaties.

Eis 4 Voor IPv6 krijgt de Aangesloten Organisatie een reeks IPv6-adressen van Logius conform het Overheidsbreed IPv6-nummerplankader. Koppelnetswerken krijgen een IPv6-reeks voor Koppelnetswerkenspecifieke doeleinden.

Beschikbaarheid, schaalbaarheid en performance

De Koppelnetswerken van Diginetwerk en het KPS hebben een openstellingstijd van 7 x 24 uur. De beschikbaarheid is relevante SLA's vastgelegd. Verstoringen dienen ook gedurende deze periode gemeld en verholpen te worden, conform de oplostijden zoals beschreven in het DAP. De beschikbaarheid van Diginetwerk dient dermate hoog te zijn, dat afnemers ervaren dat diensten binnen het stelsel altijd beschikbaar zijn. Wijzigingen die het gehele stelsel raken worden conform de procedures in het DAP vooraf aan alle deelnemers gemeld.

Eis 5 De Koppelnetswerken van Diginetwerk en het KPS dienen een opstellingstijd te hebben van 7 x 24 uur.

Om de continue beschikbaarheid te borgen dienen Koppelnetswerken redundant en met automatische fail-over op het KPS te worden aangesloten.

Eis 6 De Koppelnetswerken dienen redundant en met automatische fail-over op het KPS aangesloten te worden.

De schaalbaarheid van Diginetwerk dient zodanig te zijn dat de vraag in groei aan capaciteit ingevuld kan worden. In beginsel zijn Diginetwerkaansluitingen van 100 Mbps en 1 Gbps leverbaar, maar dit moet kunnen doorgroeien naar 10 Gbps en hoger indien de vraag van Aangesloten Organisaties dit vereist.

Eis 7 Diginetwerkaansluitingen worden geleverd met een capaciteit van 100 Mbps, 1 Gbps, of hoger. Een Koppelnetswerk dient schaalbaar te zijn, zodat in de toekomst ook 10 Gbps of hoger geleverd kan worden.

Eisen aan de maximale vertraging in het netwerk:

- Maximale Round trip delay (RTD) in een Koppelnetswerk van aansluiting Aangesloten Organisatie tot KPS: 10 ms
- Maximale Round trip delay (RTD) binnen het KPS: 1 ms

Gemeten met een pakket van 100 Bytes bij een belasting van minder dan 80% van de maximale capaciteit van resp. aansluiting Aangesloten Organisatie en aansluiting op KPS.

Eis 8 De vertraging in Diginetwerk is maximaal 21 ms RTD van Diginetwerkaansluiting tot Diginetwerkaansluiting.

Quality of Service

Quality of Service (QoS) is een belangrijke functie om netwerken zoals Diginetwerk geschikt te maken voor verschillende verkeersstromen zoals data, spraak en video. QoS zorgt ervoor dat verschillende verkeerstypen de juiste behandeling in het netwerk krijgen. Zo is spraakverkeer veel gevoeliger voor vertraging dan video of dataverkeer. Ook heeft bulk-dataverkeer (bestandsoverdracht, replicaties, back-ups) andere behoefte dan dat interactief dataverkeer zoals bijvoorbeeld Citrix of VDI.

Bij publicatie van deze versie is Quality of Service nog niet geactiveerd door de Koppelnetswerkaanbieders en de KPS-aanbieder van Diginetwerk. QoS kan geactiveerd worden op basis van een klantvraag.

Voor een juiste werking van QoS tussen verschillende organisaties zal de inrichting afgestemd moeten worden. Deze paragraaf beschrijft de inrichting van QoS voor Diginetwerk, deze is gebaseerd op IETF-standaard RFC-4594; "Figure 3, DSCP to Service Class Mapping" ([zie](#)) en wordt veel toegepast. De QoS-inrichting voor Diginetwerk is gelijk aan die van het Rijks OverheidsNetwerk (RON), zodat QoS ook goed kan functioneren tussen op Diginetwerk en RON aangesloten organisatie.

Deze QoS-instellingen kunnen ook binnen aangesloten organisaties gebruikt worden, maar noodzakelijk is dat niet. Indien een organisatie andere instellingen gebruik zal er op het koppelveld met Diginetwerk, de Diginetwerkaansluiting, mogelijk een vertaalslag gemaakt moeten worden.

Eis 9 Voor Diginetwerk wordt QoS uitsluitend afgestemd voor verkeersstromen tussen de Diginetwerkaansluitingen van Aangesloten Organisaties. De Diginetwerk QoS-standaard kan ook binnen een Aangesloten Organisatie gebruikt worden, maar dat is niet verplicht.

De implementatie van QoS bestaat uit het classificeren en markeren van verkeer en het toepassen van QoS-bewerkingen op tussenliggende netwerkkaparaatuur, gebaseerd op deze QoS-markering. Classificeren en QoS-markering worden over het algemeen bij voorkeur zo dicht mogelijk bij de bron uitgevoerd, bijvoorbeeld op de aangesloten apparatuur (PABX, videoconferentiesets), of door de gebruikte applicaties. Dit maakt verkeer direct herkenbaar, zodat een verkeersstroom end-to-end voordeel kan hebben van QoS.

Het classificeren en markeren van verkeer is een verantwoordelijkheid van de aangesloten organisatie. Diginetwerk speelt daar geen rol in. Koppelnetswerken kunnen QoS-classificatie en -markering als dienst aanbieden voor Aangesloten organisaties.

Eis 10 Aangesloten organisaties zijn verantwoordelijk voor de correcte QoS-classificatie en markering van hun verkeersstromen op de Diginetwerkaansluiting. Koppelnetswerken kunnen QoS-classificatie en -markering als dienst aanbieden op de Diginetwerkaansluiting.

Indien een Koppelnetswerk de QoS-bewerkingen zoals in deze paragraaf beschreven (nog) niet ondersteunt zal dit Koppelnetswerk aangeboden QoS-markeringen transparant en zonder aanpassingen transporteren. Dit zorgt ervoor dat de QoS-markering van het verkeer herkenbaar blijft en in andere Koppelnetswerken gebruikt kan worden.

Eis 11 De Koppelnetswerken zullen QoS-bewerkingen conform deze specificatie toepassen en als het Koppelnetswerk QoS (nog) niet ondersteunt zal het Koppelnetswerk de QoS-markeringen transparant transporteren.

Het Diginetwerk QoS-model is gebaseerd op Diffserv en volgt RFC4594. In deze RFC wordt een aanbeveling voor mapping van applicaties, service-klassen en DiffServ Code Points oftewel DSCP's beschreven. Deze DiffServ Code Points vormen de markering waarmee de QoS-klasse van een verkeersstroom aangegeven wordt.

Voor Diginetwerk wordt het aantal serviceklassen beperkt tot vier klassen voor gebruikersverkeer en één Network Control-klasse voor beheer/management van het netwerk. Dit is een veel gebruikt model, enerzijds omdat apparatuur regelmatig niet meer klassen ondersteunt, anderzijds om het beheer eenvoudig te houden. De volgende vijf serviceklassen die voor Diginetwerk gebruikt zullen worden zijn:

- Network Control
- Spraak

- Video
- Bulk
- Standaard

Andere serviceklassen/verkeersstromen zullen in eerste instantie ingedeeld worden in Spraak, Video, Bulk of Standaard-klasse. Het opnemen van een extra serviceklasse kan als doorontwikkelingsverzoek worden aangemeld bij Logius.

Service Class Name	DSCP Name	Application Examples	Diginetwerk-naam
Network Control	CS6	Network routing	Network Control
Telephony	EF	IP Telephony bearer	Spraak
Signaling	CS5	IP Telephony Signaling	-
Multimedia Conferencing	AF41, AF42, AF43	H.323/V2 video conferencing (adaptive)	Video
Real-Time Interactive	CS4	Video conferencing and Interactive gaming	-
Multimedia Streaming	AF31, AF32, AF33	Streaming video and audio on demand	-
Broadcast Video	CS3	Broadcast TV& live events	-
Low-Latency Data	AF21, AF22, AF23	Client-server transactions Web-based ordering	-
OAM	CS2	OAM&P	-
High-Throughput Data	AF11, AF12, AF13	Store and forward applications	Bulk
Standard	DF (CS0)	Undifferentiated applications	Standaard
Low-Priority Data	CS1	Any flow that has no BW assurance	-

Tabel 1: QOS-indeling RFC4594 - DSCP to Service Class Mapping, met **vetgedrukt** de voor Diginetwerk gereserveerde klassen met de Diginetwerk-naamgeving.

Eis 12 Diginetwerk maakt naast de standaard Network Control-klasse gebruik van de vier QoS-klassen: Spraak, Video, Bulk en Standaard. De Videoklasse wordt tevens gebruikt voor Citrix en VDI-verkeer. De verkeersklassen zijn herkenbaar aan de DSCP-codering zoals in Tabel 1 beschreven.

De Koppelnetswerken zorgen er met hun QoS-bewerkingen voor dat verkeer in een bepaalde verkeersklasse behandeld wordt zodat dit resulteert in acceptabele bandbreedte, delay, jitter en packetloss voor de betreffende verkeersstroom. Om QoS end-to-end te laten functioneren zullen Aangesloten organisaties er ook in hun netwerk voor moeten zorgen dat elke verkeersstroom een behandeling krijgt die resulteert in acceptabele bandbreedte, delay, jitter en packetloss.

Op het Diginetwerkkoppelvlak met de Aangesloten organisatie geldt dat per klasse een minimale bandbreedte gereserveerd kan worden. In tabel 2 is hiervan een voorbeeld gegeven. Hierbij geldt steeds dat als de gereserveerde bandbreedte binnen een klasse niet volledig gebruikt wordt, deze bandbreedte ter beschikking komt van de andere klassen. Dus als er bijvoorbeeld geen verkeer in de overige klassen gebruikt wordt, dan kan de Bulk-klasse zelfs volledige bandbreedte van de verbinding gebruiken. Als alle klassen volledig gebruikt worden blijft nog 5% van de bandbreedte over voor Bulk-verkeer.

Klasse	QoS-markering (DSCP Code)	Bandbreedte koppelvlak (voorbeeld)
Spraak	EF	5%
Video (incl. VDI, Citrix)	AF41/AF42/AF43	20%
Standaard	Overige DSCP waarden	70%
Bulk	AF11/AF12/AF13	5%
Totaal		100%

Tabel 2: Voorbeeld verkeersklasse en QoS markering op basis van DSCP-code

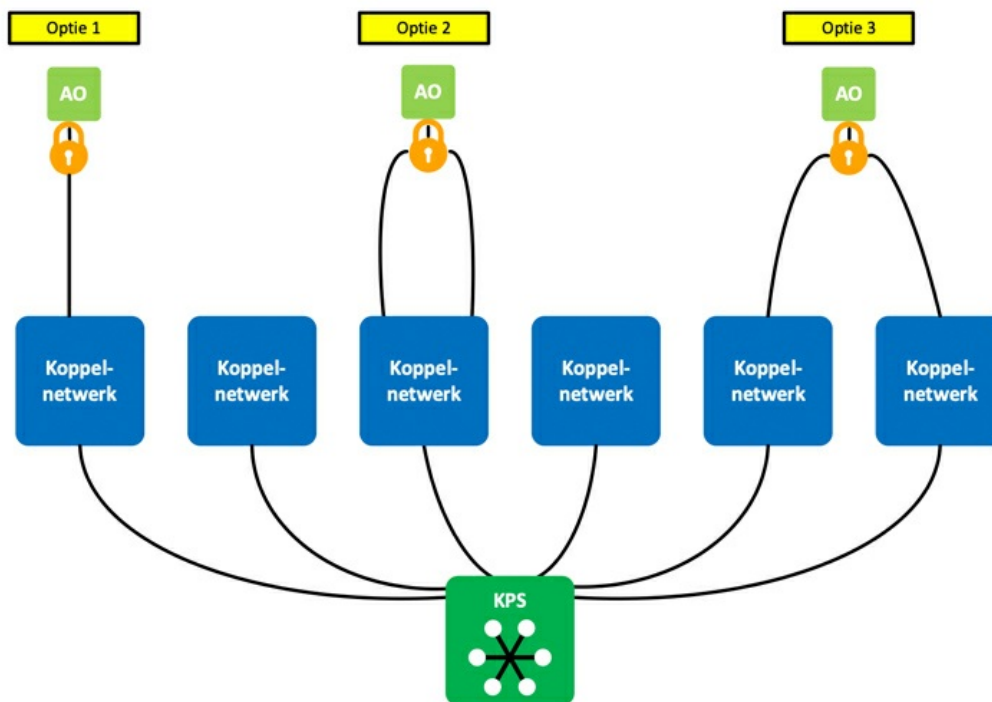
Eis 13 Op het Diginetwerkkoppelvlak met de Aangesloten organisatie is het mogelijk aan elke klasse een minimale hoeveelheid bandbreedte toe te delen. Als deze bandbreedte niet benut wordt, kan deze door verkeer in de andere klassen gebruikt worden.

Koppelvlak Aangesloten Organisatie - Koppelnetswerk

De specificaties van de aansluitingen van Aangesloten Organisaties (type stekker/connector, glas, koper, bandbreedte) kunnen variëren bij de verschillende Koppelnetswerken. Koppelnetswerken dienen zowel enkelvoudige als redundante aansluitingen op het Koppelnetswerk te kunnen leveren. Organisaties mogen ook een redundante aansluiting realiseren door op twee Koppelnetswerken te koppelen, indien dit door de betrokken Koppelnetswerken ondersteund wordt.

Eis 14 De klantaansluitingen en koppelvlakken zijn gebaseerd op gebruikelijke glas- en koperinterfaces. De aansluitingen hebben een capaciteit van minimaal 100 Mbps. Op OSI-model laag 1 worden interfaces op koper en glas aangeboden, op laag 2 Ethernet en op laag 3 IP.

Koppelnetswerken dienen zowel enkelvoudige (optie 1) als redundante Diginetwerkaansluitingen (optie 2) op het Koppelnetswerk te kunnen leveren. Organisaties mogen ook een redundante aansluiting realiseren door op twee verschillende Koppelnetswerken te koppelen (optie 3), indien dit door de betrokken Koppelnetswerken ondersteund wordt. De drie opties voor Diginetwerkaansluitingen zijn in onderstaande tekening weergegeven:



Figuur 3: Aansluitopties voor Aangesloten Organisaties op Koppeln-netwerken

Eis 15 Koppeln-netwerken dienen zowel enkelvoudige als redundante Diginetwerkaansluitingen op het Koppeln-netwerk te kunnen leveren. Organisaties mogen ook een redundante aansluiting realiseren door op twee verschillende Koppeln-netwerken te koppelen, indien dit door de betrokken Koppeln-netwerken ondersteund wordt.

Een redundante aansluiting van een organisatie op twee verschillende Koppeln-netwerken biedt voordelen ten aanzien van risicospreiding. Dit wordt ook wel een Multihomed-aansluiting genoemd. Voor dit type aansluiting gelden enkele specifieke eisen ten aanzien van de benodigde IPv4-adressen en het gebruik en configuratie van het BGP-protocol. Hierdoor kan de Aangesloten Organisatie zelf het netwerkverkeer sturen via één van zijn Koppeln-netwerkaanbieders.

Voor het opzetten van een multihomed aansluiting is een infokaart beschikbaar die is gepubliceerd op de Samenwerkrumte Diginetwerk.

Eisen

- Deze aansluiting wordt uitsluitend gemaakt op basis van het BGP-routeringsprotocol
- De Aangesloten Organisatie beschikt over de benodigde kennis van het BGP-protocol.
- De Aangesloten Organisatie krijgt van Logius een voor dit doel gereserveerde koppeln-netwerkonafhankelijke IPv4-reeks toegekend. Er wordt hier geen gebruik gemaakt van IPv4-adressen uit de pool van de Koppeln-netwerkaanbieder. Voor IPv6 heeft de AO per definitie een eigen unieke IP-reeks.
- De Aangesloten Organisatie gebruikt de BGP-attributen AS-Path prepending en Local preference voor route manipulatie.
- De Aangesloten Organisatie maakt gebruik van een uniek BGP AS-nummer (public, of private door Logius uitgegeven).
- De Koppeln-netwerkaanbieder accepteert op de Diginetwerkaansluiting de specifieke IPv4-reeks van de AO in de BGP-prefixlist, en routeert deze door binnen zijn Koppeln-netwerk.
- De Koppeln-netwerkaanbieder voert geen route-summarization uit voor deze specifieke IP-prefix op de koppeling met KPS.
- De Koppeln-netwerkaanbieder past geen AS-path-informatie aan voor deze specifieke IP-prefix binnen het Koppeln-netwerk of op de koppeling met KPS

Eis 16 Redundante aansluitingen op twee verschillende Koppeln-netwerken (Multihomed aansluiting) dienen te voldoen aan additionele eisen ten aanzien van het gebruik van koppeln-netwerkonafhankelijke IPv4-adressen en specifieke BGP-configuratie-instellingen.

De Stelselregisseur stelt de aansluitvoorwaarden voor het Afsprakenstelsel Diginetwerk op. Door het ondertekenen van aansluitvoorwaarden en de overeenkomsten worden alle aangesloten organisaties en de koppeln-netwerkaanbieders gehouden aan de gestelde eisen om de goede en veilige werking van Diginetwerk te waarborgen.

De aangesloten organisaties en de koppeln-netwerken zijn zelf verantwoordelijk voor het naleven van de afspraken en de verantwoording hierover.

Eis 17 Elke Aangesloten Organisatie voldoet aan de aansluitvoorwaarden Diginetwerk.

Koppelvvlak Koppeln-netwerk-KPS

In deze paragraaf staan de technische specificaties benoemd waaraan het koppelvvlak tussen Koppeln-netwerk en het KPS minimaal moet voldoen.

Het koppelvvlak tussen een Koppeln-netwerk en het KPS is gebaseerd op de gebruikelijke netwerkstandaarden en snelheden. Op laag 1 worden interfaces op standaard op single-mode glas aangeboden en optioneel op multi-mode en koper. Op laag 2 op Ethernet en op laag 3 op IP. Koppeln-netwerkaanbieders en de KPS-leverancier mogen additionele standaarden overeenkomen. Logius kan de set minimaal te ondersteunen standaarden aanpassen als er vraag naar is (bijvoorbeeld hogere bandbreedte).

In onderstaande tabel zijn de interface-opties van KPS weergegeven.

Aansluiting KPS	Interface-opties
1 Gbps	- Single Mode (1G-LX) - Multi-mode (1G-SX) - Koper (1G-T)
10 Gbps	- Single Mode (10G-LR) - Multi-mode (10G-SR)
40/100 Gbps	- Single Mode (40/100G-LR4) - Multi-mode (40/10G-SR4)

Opmerkingen bij bovenstaande tabel:

- **Single-mode:** standaard
- **Multi-mode:** op speciaal verzoek
- **Koper/100Mbps:** op speciaal verzoek, geleverd op 1GE Koper; legacy, alleen t.b.v. backward-compatibiliteit.

Het koppelvlak tussen een Koppelnetwork en een KPS is gebaseerd op de gangbare netwerkstandaarden en snelheden, zoals vermeld in Tabel 1 genoemde standaarden. Op OSI-laag 1 worden interfaces standaard op single-mode glas aangeboden en optioneel op multi-mode en koper. Op OSI-laag 2 op Ethernet en op OSI-laag 3 op IP. In alle gevallen wordt gebruik gemaakt van auto-negotiate en full duplex.

De Koppelnetworken dienen Ethernet-frames met een MTU van minimaal 1500 bytes kunnen transporteren, bij voorkeur wordt een MTU van 9000 bytes ondersteund. KPS ondersteunt standaard een MTU van 9000 bytes.

Eis 19 Koppelnetworken ondersteunen minimaal een Ethernet MTU van 1500 bytes en bij voorkeur een Ethernet MTU van 9000 bytes. KPS ondersteunt standaard een Ethernet MTU van 9000 bytes.

Routing op het koppelvlak tussen een Koppelnetwork en KPS is dynamisch en gebaseerd op BGP-4. Hierbij wordt gebruik gemaakt van publieke AS-nummers die uitgegeven zijn door het RIPE NCC. Indien dit voor een Koppelnetworkaanbieder niet mogelijk is, kan gebruikt gemaakt worden van private AS-nummers die door Logius worden uitgegeven en geregistreerd. Een Koppelnetwork en het KPS dienen zowel het gebruik van 16-bit als 32-bit AS-nummers te ondersteunen.

Eis 20 Routing op het koppelvlak tussen een Koppelnetwork en het KPS is gebaseerd op BGP-4 en gebruikt door RIPE NCC of Logius geregistreerde AS-nummers. Zowel 16-bit als 32-bit AS-nummers dienen ondersteund te worden.

Om de IP-routingtabel op Diginetwerk compact te houden wordt route-summarization toegepast door de Koppelnetworkaanbieder op de router verbonden met KPS. Een Koppelnetwork adverteert altijd het grootst mogelijke subnet (dus de kleinst mogelijke prefix) naar de KPS-route-servers, dat is toegewezen of is toegestaan om te adverteren met het juiste AS-pad van AS-nummers die door RIPE NCC of Logius zijn geregistreerd. Een grote (lange) prefix is een klein subnet en een groot subnet vereist een kleine prefix. Een koppelnetwork adverteert geen more-specific prefixen naar de route-servers van het KPS. Uitzondering hierop zijn more-specific prefixen uit de aparte reeks die voor Multi-homed-aansluitingen is vastgesteld.

De maximale prefix-length van een IPv4-subnet dat wordt geadverteerd naar KPS is een /29 (daarmee geldt dat /30,/31,/32 niet zijn toegestaan). De maximale prefix-length van een IPv6-prefix die wordt geadverteerd is een /64 (daarmee geldt dat /65-/128 niet zijn toegestaan).

Eis 21 Koppelnetworkaanbieders passen route-summarization toe op de prefixen die naar KPS worden geadverteerd. Een Koppelnetwork adverteert altijd het grootst mogelijke prefix naar de KPS-route-servers. De maximale prefix-length voor IPv4 is /29, voor IPv6 is dat /64.

De KPS-beheerder stelt op de KPS-route-servers prefix-filters in, zodat alleen de toegewezen/toegestane prefixen van een Koppelnetwork door KPS worden geaccepteerd. Hiermee wordt voorkomen dat een Koppelnetwork een prefix toegewezen aan een ander Koppelnetwork kan adverteren en daarmee BGP-hijacking op Diginetwerk veroorzaakt.

Voor het maximaal aantal prefixes dat op het koppelvlak met KPS wordt ontvangen, kunnen koppelnetworkbeheerders de functie *maximal prefix limit* instellen ter bescherming van het routing domein en de aangesloten routers binnen het koppelnetwork. Het gebruik van de functie *maximal prefix limit* is afhankelijk van de architectuur binnen het koppelnetwork en de toegepaste netwerkcomponenten. De functie is niet verplicht en dient minimaal op 2000 te worden gezet als die wordt toegepast. Daarnaast wordt de restart functie ingesteld om te zorgen dat de BGP-sessie automatisch herstart wordt indien de limiet wordt overschreden.

Eis 22 Koppelnetworkbeheerders stellen optioneel een *maximal prefix limit* in op het koppelvlak met KPS. De *maximal prefix limit* wordt minimaal op 2000 prefixes ingesteld. De restart functie *maximal prefix limit* wordt ingesteld op maximaal 5 minuten om te waarborgen dat de BGP-sessie automatisch wordt herstart.

De Koppelnetworkaanbieder is verantwoordelijk voor de verbinding van het Koppelnetwork naar het KPS. De Koppelnetworkaanbieder plaatst zijn router, onder begeleiding van de KPS-leverancier in de kasten van het KPS, welke voorzien zijn van 2 onafhankelijke spanningsgroepen. De apparatuur dient te passen binnen de daarvoor toegewezen ruimte van max. 4 hoogte-eenheden en moet verbonden worden met een vrije positie op het patchpaneel (koper of glas). De KPS-leverancier kan daarna de koppeling met het KPS realiseren op afstand, of door het aanbrengen van een patchverbinding. Andere aansluitopties kunnen in overleg met de KPS-aanbieder en Logius worden besproken.

Eis 23 Koppelnetworkaanbieders plaatsen hun netwerkapparatuur, waaronder ten minste een IP-router, in de kasten van het KPS. De beschikbare ruimte is max. 4 standaard hoogte-eenheden (4 x 44,45mm). Andere aansluitopties kunnen in overleg met de KPS-aanbieder en Logius worden besproken.

De Koppelnetworkaanbieder dient op elke KPS-locatie een IP-router te plaatsen en te verbinden met het OSI-laag 2 KPS-netwerk. De IP-adressen voor de koppeling wordt door de KPS-leverancier uit naam van Logius toegewezen. Op elke KPS-aansluitpoort wordt maximaal één MAC-adres toegelaten.

Eis Koppelnetwerkenaanbieders plaatsen op iedere KPS-locatie een IP-router voor de koppeling met KPS. Het IP-adres wordt toegewezen door de KPS-leverancier. Er wordt per aansluitpoort maximaal één MAC-adres toegelaten.

De Stelselregisseur stelt de aansluitvoorwaarden voor het Koppelnets Publieke Sector op. Met de ondertekening van de aansluitvoorwaarden en de overeenkomsten worden alle koppelnetwerkenaanbieders gehouden aan de gestelde eisen om de goede en veilige werking van Diginetwerk te waarborgen.

De koppelnetwerken zijn zelf verantwoordelijk voor het naleven van de afspraken en de verantwoording hierover.

Eis 25 Elke Koppelnetwerk voldoet aan de aansluitvoorwaarden Koppelnets Publieke Sector.

Beveiliging

Het basisbeveiligingsniveau van het Afsprakenstel Diginetwerk is een semi-vertrouwde zone conform de definitie in de [NORA](#).

Eis 26 Binnen Diginetwerk is het basisbeveiligingsniveau semi-vertrouwd.

De Aangesloten Organisatie die op een of meer Koppelnetwerken een Diginetwerkaansluiting afneemt, dient de aansluiting(en) via een beveiligd koppelvlak zelf te termineren, ongeacht of het bedrijfsnetwerk van de AO een gelijk, hoger of lager beveiligingsniveau heeft.

Eis 27 Een Aangesloten Organisatie die een Diginetwerkaansluiting afneemt, dient de aansluiting op een beveiligd koppelvlak te termineren.

De Aangesloten Organisatie beveiligt zijn netwerk en aansluiting op een Koppelnetwerk conform de informatiebeveiligingsstandaarden zoals beschreven in de BIO, of NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002 indien het geen Overheidsorganisatie betreft.

Eis 28 Aangesloten Organisaties die op een van de koppelnetwerken van Diginetwerk aansluiten dienen hun netwerk en aansluiting op het Koppelnetwerk te beveiligen conform de BIO of NEN-ISO/IEC 27001/NEN-ISO/IEC 27002 standaarden indien het geen Overheidsorganisatie betreft.

Om het besloten karakter van Diginetwerk te garanderen mag op Diginetwerk alleen IP-verkeer gerouteerd worden afkomstig van IP-adressen die door Logius voor Diginetwerk zijn vastgesteld en geregistreerd. Het nummerplan Diginetwerk met de vastgestelde IP-adressen is gepubliceerd op de Samenwerkruimte Diginetwerk.

Indien een Koppelnetwerkenaanbieder verkeer met van dit nummerplan afwijkende IP-adressen aantreft, dient dit onmiddellijk gerapporteerd te worden aan Logius.

Eis 26 Binnen Diginetwerk mag alleen IP-verkeer gerouteerd worden afkomstig van IP-adressen die door Logius voor Diginetwerk zijn vastgesteld en geregistreerd. Indien onbekend en/of onvertrouwd verkeer in Diginetwerk aangetroffen wordt door een Koppelnetwerkenaanbieder, dient dit onmiddellijk aan Logius gerapporteerd te worden.

Diginetwerk is verder transparant voor IP-verkeer met adressen in de voor Diginetwerk vastgestelde IP-reeksen. Dit wil zeggen dat het KPS en Koppelnetwerken IP-verkeer transparant moeten doorgeven en geen protocollen of IP-adressen binnen de vastgestelde IP-reeksen mogen blokkeren of uitsluiten. Verkeer dat buiten vastgestelde Diginetwerk IP-reeksen valt, moet wel geblokkeerd worden.

Alleen de Aangesloten Organisaties mogen onderscheid aanbrengen welke andere organisaties hun diensten mogen afnemen. De aanbiederende Organisatie mag hiervoor maatregelen toepassen zoals IP- of poortfiltering, authenticatie en autorisatiefiltering.

Eis 27 KPS en de Koppelnetwerken van Diginetwerk zijn transparant voor IP-verkeer met adressen in de voor Diginetwerk vastgestelde IP-reeksen [6]. Adressen buiten deze reeksen worden geblokkeerd. Aangesloten Organisaties mogen wel filtermaatregelen nemen voor de Diginetwerk IP-reeksen en blokkeren ook onbekend IP-verkeer.

Een belangrijke functie van Diginetwerk is het transparant overbrengen van IP-pakketten tussen Diginetwerkaansluitingen. Hierom mogen er tussen de Koppelnetwerken en KPS en op de Diginetwerkaansluiting van het Koppelnetwerk naar de Aangesloten Organisatie geen blokkerende firewalls of IP-filters aanwezig zijn voor de afgesproken Diginetwerk IP-reeksen [6]. Transport van IP-pakketten met vastgestelde IP-adressen wordt transparant doorgelaten.

Eis 28 Tussen de Koppelnetwerken en KPS en op de Diginetwerkaansluiting van het Koppelnetwerk naar de Aangesloten Organisatie mogen geen blokkerende firewalls of IP-filters aanwezig zijn voor de afgesproken Diginetwerk IP-reeksen. Transport van IP-pakketten met vastgestelde IP-adressen wordt transparant doorgelaten.

Om het besloten karakter van Diginetwerk te garanderen mag op Diginetwerk alleen IP-verkeer gerouteerd worden afkomstig van IP-adressen die door Logius voor Diginetwerk zijn vastgesteld en geregistreerd. Het nummerplan Diginetwerk met de vastgestelde IP-adressen is gepubliceerd op de Samenwerkruimte Diginetwerk.

Indien een Koppelnetwerkenaanbieder verkeer met van dit nummerplan afwijkende IP-adressen aantreft, dient dit onmiddellijk gerapporteerd te worden aan Logius.

Eis 29 Binnen Diginetwerk mag alleen IP-verkeer gerouteerd worden afkomstig van IP-adressen die door Logius voor Diginetwerk zijn vastgesteld en geregistreerd. Indien onbekend en/of onvertrouwd verkeer in Diginetwerk aangetroffen wordt door een Koppelnetwerkenaanbieder, dient dit onmiddellijk aan Logius gerapporteerd te worden.

Diginetwerk is verder transparant voor IP-verkeer met adressen in de voor Diginetwerk vastgestelde IP-reeksen. Dit wil zeggen dat het KPS en Koppelnetwerken IP-verkeer transparant moeten doorgeven en geen protocollen of IP-adressen binnen de vastgestelde IP-reeksen mogen blokkeren of uitsluiten. Verkeer dat buiten vastgestelde Diginetwerk IP-reeksen valt, moet wel geblokkeerd worden.

Alleen de Aangesloten Organisaties mogen onderscheid aanbrengen welke andere organisaties hun diensten mogen afnemen. De aanbiederende Organisatie mag hiervoor maatregelen toepassen zoals IP- of poortfiltering, authenticatie en autorisatiefiltering.

Eis 30 KPS en de Koppelnetwerken van Diginetwerk zijn transparant voor IP-verkeer met adressen in de voor Diginetwerk vastgestelde IP-reeksen. Adressen buiten deze reeksen worden geblokkeerd.

Aangesloten Organisaties dienen filtermaatregelen te nemen om onbekend IP-verkeer (zijnde niet-Diginetwerk IP adressen) te filteren.

Een belangrijke functie van Diginetwerk is het transparant overbrengen van IP-pakketten tussen Diginetwerkaansluitingen. Hierom mogen er tussen de Koppelnetwerken en KPS en op de Diginetwerkaansluiting van het Koppelnetwerk naar de Aangesloten Organisatie geen blokkerende firewalls of IP-filters aanwezig zijn voor de afgesproken Diginetwerk IP-reeksen. Transport van IP-pakketten met vastgestelde IP-adressen wordt transparant doorgelaten.

Eis 31 Tussen de Koppelnetwerken en KPS en op de Diginetwerkaansluiting van het Koppelnetwerk naar de Aangesloten Organisatie mogen geen blokkerende firewalls of IP-filters aanwezig zijn voor de afgesproken Diginetwerk IP-reeksen. Transport van IP-pakketten met vastgestelde IP-adressen wordt transparant doorgelaten.

Eis 32 heeft tot gevolg dat Koppelnetwerkaanbieders verplicht zijn om uitgaand verkeer naar het KPS te controleren op source IP-adressen en pakketten met een source IP-adres dat niet tot het vastgestelde IP-nummerplan Diginetwerk behoort. Indien er afwijkende IP-adressen zijn aangetroffen dient het verkeer met die adressen verwijderd te worden, zogenaamde anti-spoofing protectie. De KPS-aanbieder zorgt ervoor dat geen IP-routes/prefixes geïnjecteerd en gerouteerd worden die buiten de vastgestelde IP-reeksen vallen

Eis 32 Koppelnetwerkaanbieders zijn verplicht anti-spoofing protectie toe te passen op hun koppelvlak met het KPS.

Eis 33 De KPS-aanbieder zorgt ervoor dat er geen IP routes/prefixes in BGP geïnjecteerd of verspreid worden die niet behoren tot de vastgestelde IP-adressen van Diginetwerk.

Beheer

Vanwege het stelselkarakter van Diginetwerk zijn heldere afspraken over het beheer noodzakelijk. Er zijn vaak meerdere partijen bij een wijziging of incident betrokken. In het Dossier Afspraken en Procedures Diginetwerk [4] zijn de processen beschreven. In deze paragraaf worden enkele beheereisen vanuit de architectuur beschreven.

Omdat in het Afsprakenstelsel Diginetwerk meerdere partijen bij beheer betrokken zijn, is het essentieel dat de verschillende partijen gezamenlijk een goed inzicht en overzicht hebben van de status van netwerken, diensten en componenten die samen de Diginetwerkinfrastructuur vormen. Logius heeft hiertoe centrale beheertools ingericht, welke door de Aangesloten Organisaties, Koppelnetwerkaanbieders en de KPS-aanbieder gebruikt kunnen worden. Essentieel voor het goed functioneren van deze tooling is het kunnen vergaren van informatie van diverse componenten in de Diginetwerk-keten.

Hiervoor wordt door Logius met de KPS-leverancier en Koppelnetwerkaanbieders een aantal routers of testsystemen bepaald die middels probes gepolled worden met netwerkprotocollen, waaronder ping, TCP-connect, SNMP en HTTP-queries. Aangesloten Organisaties kunnen op verzoek ook in overleg met Logius systemen aan de beheertools toe laten voegen.

Eis 34 Koppelnetwerkaanbieders en de KPS-leverancier verplichten zich de centrale beheertools van Logius van adequate informatie te voorzien. Hiervoor worden in overleg met Logius routers en testsystemen bepaald die vanuit probes gepolled worden netwerkprotocollen, waaronder ping, TCP-connect, SNMP en HTTP-queries.

Informatie over de routing en beschikbare prefixes is essentieel bij het oplossen van incidenten. Hiertoe zullen Koppelnetwerkaanbieders en de KPS-aanbieder een "BGP looking glass"-dienst leveren. Deze looking glass-tool geeft inzicht in de BGP-routing, ping- en traceroute-gegevens binnen Diginetwerk, gezien vanuit het Koppelnetwerk of KPS.

Eis 35 Koppelnetwerkaanbieders en de KPS-leverancier geven inzicht in de Diginetwerk-BGP-routing, ping- en traceroute gegevens, door middel van BGP looking glass-tools die toegankelijk zijn voor alle deelnemers in het stelsel.

In de Koppelnetwerken en in het KPS zijn test-websites beschikbaar, waar een http-sessie naar toe gemaakt kan worden. Deze site geeft het IP-adres terug van de initiator.

Eis 36 Koppelnetwerkaanbieders en de KPS-leverancier stellen in hun netwerkdeel van de Diginetwerkinfrastructuur een testwebsite beschikbaar waar een http-sessie naar toe gemaakt kan worden.

Voor beheer is het belangrijk dat alle deelnemers aan het Afsprakenstelsel Diginetwerk (Koppelnetwerken en Aangesloten Organisaties) het pad waarover gerouteerd wordt (met traceroute) en de maximale MTU (met Path MTU Discovery, PMTUD) kunnen bepalen. Deelnemers aan het stelsel dienen de hiervoor benodigde protocollen te ondersteunen en toe te laten tot aan het systeem wat direct aan Diginetwerk is aangesloten.

Eis 37 Koppelnetwerken en Aangesloten Organisaties dienen maatregelen te nemen waarmee traceroute en PMTUD volledig ondersteund worden tot aan het systeem wat direct aan Diginetwerk is aangesloten.

5. Referenties

- [1] Nederlandse Overheid Referentie Architectuur
- NORA is gepubliceerd op de website: https://www.noraonline.nl/wiki/NORA_online
- [2] Aansluitvoorwaarden Diginetwerk
- [3] Aansluitvoorwaarden Koppelnat Publieke Sector
- [4] Dossier Afspraken en Procedures Diginetwerk
- [5] Overheidsbreed IPv6-nummerplankader

- De documenten 2-5 zijn gepubliceerd op de Logius-website: <https://www.logius.nl/diensten/diginetwerk/documentatie>
- [6] Diginetwerk IPv4 en IPv6-adressen
- Het IP-nummerplan Diginetwerk voor IPv4 en IPv6 is gepubliceerd op de besloten samenwerkruimte Diginetwerk: <https://www.samenwerkruimten.nl/teamsites/diginetwerk/Documenten>
- [7] Infokaart Multihomed aansluiting AO op Diginetwerk
 - <https://www.samenwerkruimten.nl/teamsites/diginetwerk/Documenten>

6. Afkortingen

Terminologie die in dit document zijn gebruikt.

Term	Uitleg
AO	Aangesloten Organisatie
AoD	Aansluiting op Diginetwerk
AS-nummer	Autonomous System-nummer
BGP	Border Gateway Protocol
BIO	Baseline Informatiebeveiliging Overheid. Een gemeenschappelijk normenkader, gebaseerd op de internationale norm ISO 27001/2 voor de beveiliging van de informatie(systemen) van de overheid;
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
FQDN	Fully Qualified Domain Name
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISO/IEC	International Organization for Standardization / International Engineering Consortium
KPS	Koppelnets Publieke Sector
NORA	Nederlandse Overheid Referentie Architectuur
ODC	OverheidsDataCenter
OSB	OverheidsServiceBus
PKI	Public Key Infrastructure
QoS	Quality of Service
RINIS	Routeringsinstituut (inter)nationale informatiestromen
RIPE	Réseaux IP Européens
RON	Rijksoverheidsnetwerk
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNO	Service Niveau Overeenkomst
Testa	Trans European Services for Telematics between Administrations
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network
ZBO	Zelfstandig bestuursorgaan

Website url: <https://www.logius.nl>

Print datum: 23/05/2025 06:54:57