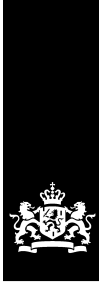


Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Diginetwerk
Architectuurdocument

Versie 1.4

8 mei 2019

Publicatie
De meest actuele versie is gepubliceerd op de Logius website onder Diginetwerk: https://www.logius.nl/diensten/diginetwerk

Inhoudsopgave

1 Inleiding

1.1 Doel van dit document

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

1.2 Scope

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

1.3 Status

Het voorliggend architectuurdocument wordt voorgelegd aan de koppelnetwerkleveranciers. De definitieve versie wordt vastgesteld door Logius. Deze versie geldt als norm voor Diginetwerk voor het geheel aan koppelnetwerken. Koppelnetwerkbeheerder, Aangesloten Organisatie en KPS dienen hun koppelnetwerken volgens deze norm in te richten.

1.4 Samenhang met andere documenten

De volgende documenten hebben een relatie tot het architectuur document van Diginetwerk: NORA, EAR en RON.

Ondanks het feit dat NORA en EAR architectuur documenten zijn voor de Rijksoverheid, hebben deze als leidraad gediend. Met name heeft NORA de beveiligingsniveaus en de aanpalende maatregelen beschreven die Diginetwerk gebruikt als uitgangsprincipes. Dit is verwoord in hoofdstuk 4.1.

In de RON documentatie wordt het RijksOverheidsNetwerk (RON) beschreven, het netwerk waarin de vier Overheids DataCenters (ODC’s) zijn geïntegreerd. Vanuit dit netwerk worden overheidsbrede diensten ontwikkeld en aangeboden aan de verschillende afnemers. Binnen RON is het Partner-I netwerk beschreven als het koppelvlak waarover de rijksoverheid communiceert met partners van de rijksoverheid. Partner-I is het netwerk van RON dat de Rijksoverheid verbindt met Diginetwerk.

2 Introductie Diginetwerk

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

2.1 Doel van Diginetwerk

Diginetwerk is een stelsel van besloten netwerken. Het doel van Diginetwerk is 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 netwerken en zonder afhankelijkheid van internet.

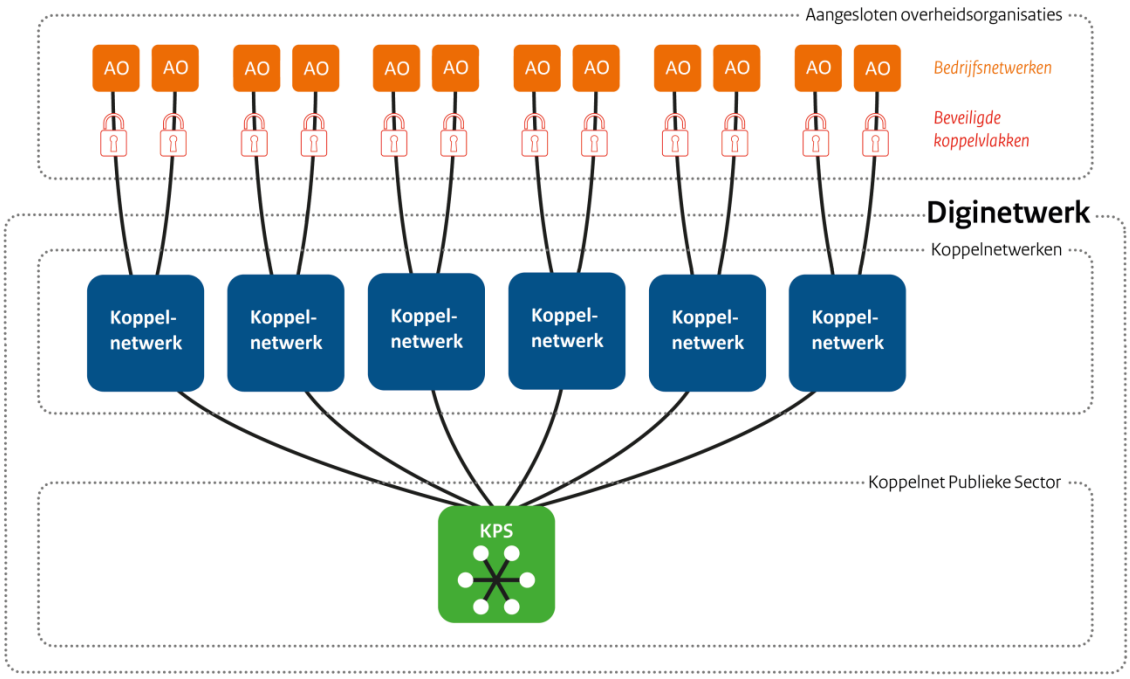
2.2 Netwerk van netwerken

In het verleden zijn er veel besloten Wide Area Netwerken door de overheid gebouwd of aanbesteed met als doel een communicatie-infrastructuur te realiseren voor een bepaalde doelgroep binnen de overheid. Voorbeelden hiervan zijn Gemnet voor de gemeentes, de Haagse Ring voor de Rijksoverheid, Suwinetwerk voor de Werk- en Inkomenketen, NAFIN voor defensie, JustitieNet voor het ministerie van Justitie en Veiligheid. Om communicatie tussen verschillende ministeries, overheden en organisaties met een publiek taak mogelijk te maken, werden veel kruisverbindingen tussen deze netwerken gelegd.

Diginetwerk is ontstaan uit het koppelen van een aantal van deze besloten netwerken voor de overheid waardoor minder kruisverbanden nodig waren en kosten bespaard konden worden. Door gemeenschappelijk afspraken te maken op het gebied van connectiviteit, beschikbaarheid, beveiliging en het gebruik van standaarden kan iedere aangesloten organisatie communiceren met een andere aangesloten organisatie.

Binnen Diginetwerk wordt een besloten netwerk een Koppelnetwerk genoemd. Al deze Koppelnetwerken zijn aangesloten op het Koppelnet Publieke Sector (KPS).

In onderstaande tekening is dit weergegeven:



Bedrijfsnetwerken van overheidsorganisaties zijn met behulp van een beveiligd koppelvlak aangesloten op één van de koppelnetwerken. De Koppelnetwerken zijn op hun beurt op het KPS gekoppeld.
Op basis van gemeenschappelijke afspraken is een stelsel ontstaan met aansluitvoorwaarden, beheer afspraken, dienstbeschrijvingen en een architectuurdocument.

In dit architectuurdocument is vastgelegd welke afspraken er op het gebied van architectuur zijn gemaakt om Diginetwerk te ontwerpen, bouwen en uit te breiden. Deze afspraken gelden voor de Koppelnetwerken, het KPS en voor de overheidsorganisaties die aangesloten zijn op Diginetwerk.

2.3 Wat zijn de voordelen voor de aangesloten organisatie?

Voor de aangesloten organisatie kan levert Diginetwerk de volgende voordelen op:

1) Door het besloten karakter is Diginetwerk een veiliger alternatief dan het open internet voor het uitwisselen van gegevens tussen overheidsorganisatie;
2) Met één netwerkaansluiting efficiënt en betrouwbaar communiceren met alle aangesloten overheidsorganisaties;
3) Systemen kunnen op een standaardwijze ingericht worden voor de koppeling met Diginetwerk. Zo bereiken organisaties een betere kwaliteit tegen lagere kosten;
4) Beschikbaarheid geborgd door een SLA;
5) Vrijheid van keuze voor een of meer Koppelnetwerken;
6) Op een eenduidige wijze diensten aanbieden en/of afnemen op Diginetwerk met andere aangesloten organisaties.

2.4 Welke rollen zijn er binnen Diginetwerk?

De volgende rollen zijn gedefinieerd binnen Diginetwerk:

1) Stelsel regisseur: Logius;
2) Koppelnetwerk: Verschillende leveranciers van een besloten overheidsnetwerk;

3) Koppelnet Publieke Sector: Koppelnet waar verschillende Koppelnetwerken verbonden worden. Nu één leverancier en in de toekomst mogelijk meer;
4) Aangesloten Organisatie: Overheidsinstelling of organisatie met een publieke taak die gebruik wil maken van Diginetwerk, om diensten af te nemen en/of te publiceren;

De Stelselregisseur (Logius) voert de regie over het Diginetwerkstelsel namens de deelnemers. Zij stelt aansluitvoorwaarden op, onderhoudt contact met de Koppelnetwerken en KPS, deelt IP-adressen en domeinnamen uit, regisseert de communicatie, dat wil zeggen het informeren koppelnetwerkbeheerders die op hun beurt hun klanten (aangesloten organisaties) informeren. Logius stelt informatie beschikbaar en vormt ook het ingangskanaal voor vragen over Diginetwerk.

De Aangesloten Organisatie is een overheidsinstelling of organisatie met een publieke taak die gebruik wil maken van Diginetwerk, om diensten af te nemen en/of aan te bieden. De Aangesloten Organisatie kan een Diginetwerk verbinding aanvragen bij één van de Koppelnetwerk leveranciers. De Aangesloten Organisatie is zelf verantwoordelijk voor het voldoen aan de aansluit-voorwaarden, het realiseren van een beveiligd koppelvlak en het routeren en gebruiken van toegewezen IP adressen op Diginetwerk.

Een Koppelnetwerk is een besloten netwerk voor organisaties in de publieke sector. Hierbij gaat om bestaande besloten overheidsnetwerken (o.m. Haagse Ring/OSB, Suwinet, Rinisnet). Daarnaast zijn er marktpartijen die een commercieel koppelnetwerk exploiteren voor het aansluiten van overheden en organisaties met een publieke taak (o.m. Gemnet-AoD en eGem). De Koppelnetwerkleveranciers bieden aan Aangesloten Organisaties een Diginetwerk aansluiting aan. De leveranciers van deze netwerken zorgen dat de Aangesloten Organisaties voldoen aan de aansluitvoorwaarden, daarnaast kunnen ze toegevoegde waarde diensten leveren zoals DNS, Email relay service, een beveiligd koppelvlak, etc. Verder zorgen de Koppelnetwerkleveranciers voor een aansluiting op het KPS, zodat de Koppelnetwerken met elkaar kunnen communiceren.

De leverancier van het KPS zorgt dat de verschillende Koppelnetwerken onderling verbonden worden en het verkeer daartussen gerouteerd kan worden.

3 Kader

3.1 Stelsel

De essentie van het gebruikte concept voor Diginetwerk is:

- Afsprakenstelsel van besloten netwerken
- Onafhankelijk van internet (besloten netwerk)
- Zoveel mogelijk hergebruik van bestaande besloten overheidsnetwerken
- Interoperabiliteit door toepassen van bewezen internetstandaarden

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

Door dit concept te hanteren is een stelsel van besloten netwerken ontstaan, waarbij elk autonoom beheerd netwerk een Koppelnetwerk genoemd wordt. Het geheel aan Koppelnetwerken en het Koppelnet Publieke Sector (KPS) vormt Diginetwerk. Elke Aangesloten Organisatie voldoet aan de gemeenschappelijke aansluitvoorwaarden Diginetwerk [2] en elk Koppelnetwerk voldoet aan de aansluitvoorwaarden Koppelnet Publieke Sector [3].

3.2 Betrokken Koppelnetwerken

Op dit moment zijn de volgende koppelnetwerken en leveranciers onderdeel van het Diginetwerk stelsel:

- Suwinet : Opdrachtgever BKWI/UWV
- eGem : Opdrachtgever eGem
- Equinix : Opdrachtgever Equinix
- Gemnet AoD : Opdrachtgever KPN Lokale Overheid
- Haagse Ring (OSB VPN) : Opdrachtgever Logius
- Rinisnet : Opdrachtgever RINIS
- RWS : Opdrachtgever RWS
- GGI-Netwerk : Opdrachtgever VNG-realisatie
- BT-Wolk : Opdrachtgever Logius

3.3 Governance

De Governance van het Diginetwerk stelsel is beschreven in het Dossier Afspraken en Procedures Diginetwerk [4].

4 Principes, uitgangspunten en ontwerpbeslissingen

4.1 Generieke Principes

NORA[1] is gebruikt als kader voor de generieke principes van Diginetwerk. Expliciet zijn de volgende afgeleide principes van NORA (de nummering van NORA is overgenomen) als uitgangspunten voor Diginetwerk van toepassing:

AP01. Diensten zijn herbruikbaar. Diginetwerk bestaat uit herbruikbare diensten (koppelnetwerken, 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.

4.2 Uitgangspunten

De volgende uitgangspunten gelden voor Diginetwerk:

UP1. Diginetwerk dient als zelfstandig besloten netwerk operationeel te kunnen blijven, zonder dat er een internet verbinding, of communicatie naar het internet noodzakelijk is;
UP2. Er wordt gebruik gemaakt van bewezen transportstandaarden die voor communicatie op het internet opgesteld zijn;
UP3. Er wordt gebruik gemaakt van aan de overheid toegekende reeks(en) publieke IPv4 en IPv6 adressen. Deze adressen worden niet op het internet geadverteerd of gerouteerd;
UP4. Er wordt gebruik gemaakt van publieke AS nummers die uitgegeven zijn door het RIPE NCC. Indien dit voor leveranciers niet mogelijk is, kan gebruikt gemaakt van private AS-nummers die door Logius worden uitgegeven en geregistreerd;
UP5. Het gebruik van VPN's op basis (encrypted) tunnels over Internet is, gezien de nagestreefde onafhankelijkheid van Internet binnen koppelnetwerken en voor klantaansluitingen niet toegestaan.

4.3 Ontwerpprincipes

Aanvullend aan de generieke principes zijn de volgende ontwerpprincipes voor Diginetwerk opgesteld:

OP1. Het netwerk kent een gesloten karakter. Er is geen directe (d.w.z. zonder beveiligde ontkoppeling) koppeling met openbare netwerken zoals internet mogelijk of aanwezig;
OP2. Er wordt gebruik gemaakt van een uniek IP nummerplan. Voor IPv4 worden publieke IP blokken van de overheid gebruikt die niet op internet gerouteerd worden. Voor IPv6 worden IP blokken gebruikt uit het Overheidsbreed IPv6-nummerplankader [5] dat Logius heeft opgesteld;
OP3. Tussen de Koppelnetwerken en het KPS wordt routering op basis van het BGP-4 protocol gebruikt.
OP4. Er moet rekening gehouden worden met de mogelijkheid van asymmetrische routering tussen de Koppelnetwerken en het KPS.
OP5. Koppelnetwerken mogen onderling alleen via een KPS communiceren, directe koppelingen tussen Koppelnetwerken zijn niet toegestaan;

OP6. Diensten op Diginetwerk worden ontsloten middels de DNS en een FQDN. Voor Diginetwerk zijn de domein diginetwerk.net, diginetwerk.nl en overheid-i.nl geregistreerd om diensten in het besloten netwerk te kunnen benaderen;

OP7. De Aangesloten Organisaties resolven diginetwerk.net, diginetwerk.nl en overheid-i.nl via een conditional forward naar de Rijks-DNS[1].

[1] Naast deze domeinen kan ook *int-gemnet.nl* nog gebruikt worden met een conditional forward. Dit domein is een historische uitzondering, aanbevolen worden om gebruik te maken van *diginetwerk.nl en overheid-i.nl* die centraal door Logius beheerd worden.

5 Vereisten

In dit hoofdstuk worden de eisen die gesteld worden aan Diginetwerk beschreven. Deze eisen gelden voor de Koppelnetwerken, Knooppunten Publieke sector(KPS) en de Aangesloten Organisaties die gezamenlijk het stelsel Diginetwerk vormen.

5.1 Functioneel

De belangrijkste functionele eis voor Diginetwerk is dat het één besloten netwerk voor de overheid moet vormen. Er mogen geen directe koppelingen met openbare netwerken plaatsvinden. Diginetwerk moet onafhankelijk van internet kunnen werken.

Eis 1: Diginetwerk is onafhankelijk van het internet.

Een gevolg van het principe van hergebruik (AP01) is dat het Diginetwerk bestaat uit een afsprakenstelsel van verschillende netwerken die in gebruik genomen zijn door de overheid. Om interoperabel te zijn dient het stelsel van netwerken een uniform karakter te hebben op het gebied van standaarden, beveiliging en dienstverlening.

Eis 2: Diginetwerk maakt gebruik van een set van principes, uitgangspunten en ontwerpbeslissingen, die in het gehele netwerk van toepassingen zijn.

Dit architectuurdocument beschrijft met principes, uitgangspunten en ontwerpbeslissingen de interoperabiliteit. Deze principes, uitgangspunten en ontwerpbeslissingen dienen bij alle Aangesloten Organisaties, Koppelnetwerken en het KPS gehanteerd te worden.

Eis 3: Diginetwerk is transparant voor IP verkeer met adressen in de voor Diginetwerk vastgestelde IP-reeksen. Adressen buiten deze reeksen worden geblokkeerd.

Dit wil zeggen dat een Koppelnetwerk of KPS IP verkeer transparant moet doorgeven en geen protocollen of IP adressen mag blokkeren of uitfilteren. Verkeer dat buiten vastgestelde Diginetwerk IP-reeksen valt moet geblokkeerd worden.
Alleen de Aangesloten Organisaties mogen onderscheid aanbrengen welke andere Organisaties hun diensten mogen afnemen. De aanbiedende Organisatie mag hiervoor maatregelen toepassen zoals IP- of poortfiltering, authenticatie en autorisatiefiltering.

Diginetwerk is een transportnetwerk dat ondersteunend is aan de primaire taak van de overheid.

Eis 4: Diginetwerk is ondersteunend aan de primaire taak 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.

5.2 Beschikbaarheid, schaalbaarheid en performance

Diginetwerk dient 7 x 24 uur beschikbaar te zijn. Verstoringen dienen ook gedurende deze periode gemeld en verholpen te worden.

Eis 5: Diginetwerk is 7 x 24 uur beschikbaar

De beschikbaarheid van Diginetwerk dient dermate hoog te zijn, dat afnemers ervaren dat diensten binnen het stelsel altijd beschikbaar zijn. Wijzigingen en onderbrekingen die het gehele stelsel raken dienen na vooraankondiging in een onderhoudsperiode uitgevoerd te worden. Koppelnetwerken dienen redundant en met automatische fail-over op het KPS aangesloten te worden.

Eis 6: De Koppelnetwerken 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 klantaansluitingen van 100 Mbps en 1 Gbps te leveren, maar dit moet kunnen doorgroeien naar 10 Gbps en hoger indien de klantvraag dit vereist.

Eis 7: Diginetwerk is schaalbaar tot klantaansluiting van 10 Gbps en hoger.

Eisen aan de maximale vertraging in het netwerk:

- Maximale Round trip delay (RTD) in een Koppelnetwerk van klantaansluiting tot KPS: 10 ms
- Maximale Round trip delay (RTD) binnen een KPS: 1 ms

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

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

QoS in Diginetwerk wordt geïmplementeerd[2] volgens RFC 4594 en de QoS klasse indeling van figuur 3 uit deze RFC. Minimaal de Telephony, Multimedia Conferencing, Multimedia Streaming, Low Latency Data en Low Priority Data klassen zullen beschikbaar moeten zijn.

Eis 9: Het QoS in Diginetwerk wordt geïmplementeerd conform RFC 4594, waarbij minimaal de Telephony, Multimedia Conferencing, Multimedia Streaming, Low Latency Data en Low Priority Data klassen beschikbaar dienen te zijn.

5.3 Koppelvlak Aangesloten Organisatie-Koppelnetwerk

De klantaansluitingen, het koppelvlakken tussen de Aangesloten Organisaties en Koppelnetwerken zijn gebaseerd op de gebruikelijke netwerkstandaarden en snelheden. Op OSI-model laag 1 worden interfaces op koper en glas aangeboden, op laag 2 Ethernet en op laag 3 IP.

[2] *Diginetwerk ondersteunt QoS nog niet end-to-end, waar QoS geïmplementeerd word zal het aan deze eis moeten voldoen.*

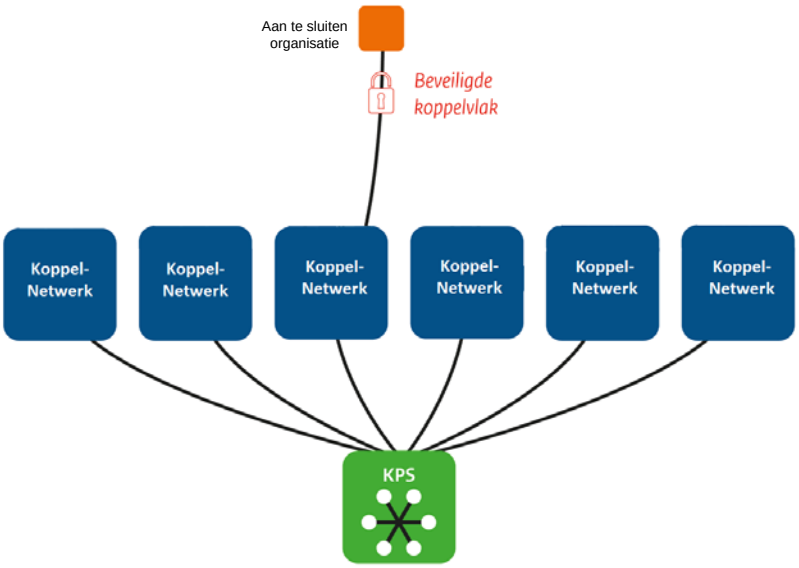
Eis 10: De klantaansluitingen en koppelvlakken tussen de Koppelnetwerken en KPS zijn gebaseerd op de gebruikelijke netwerkstandaarden en snelheden. Op OSI-model laag 1 worden interfaces op koper en glas aangeboden, op laag 2 Ethernet en op laag 3 IP.

De specificaties van de klantaansluitingen (type stekker, glas, koper, bandbreedte) kunnen variëren bij de verschillende Koppelnetwerken.

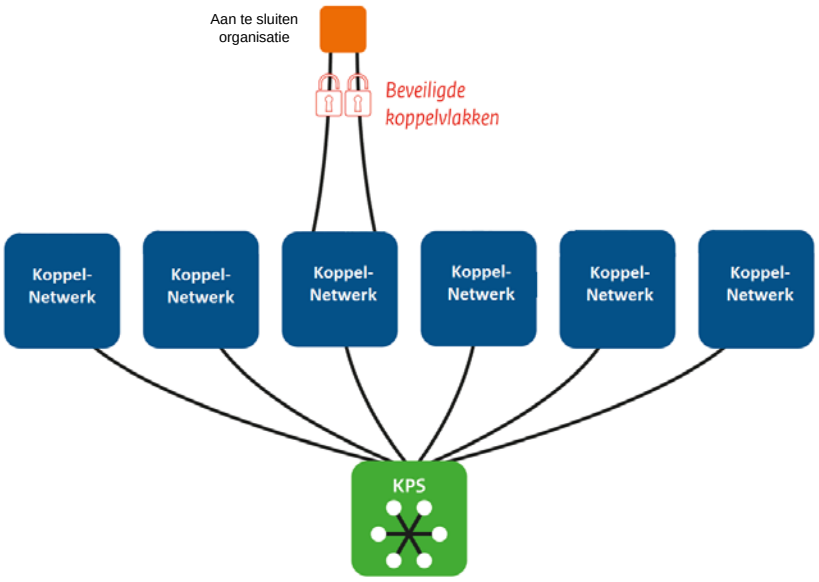
Koppelnetwerken dienen zowel enkelvoudige als redundante klantaansluitingen op het Koppelnetwerk te kunnen leveren. Organisaties mogen ook een redundante aansluiting realiseren door op twee Koppelnetwerken te koppelen, dit moet door de Koppelnetwerken ondersteund worden.

Eis 11: Koppelnetwerken dienen zowel enkelvoudige als redundante klantaansluitingen op het Koppelnetwerk te kunnen leveren. Organisaties mogen ook een redundante aansluiting realiseren door op twee Koppelnetwerken te koppelen, dit moet door de Koppelnetwerken ondersteund worden.

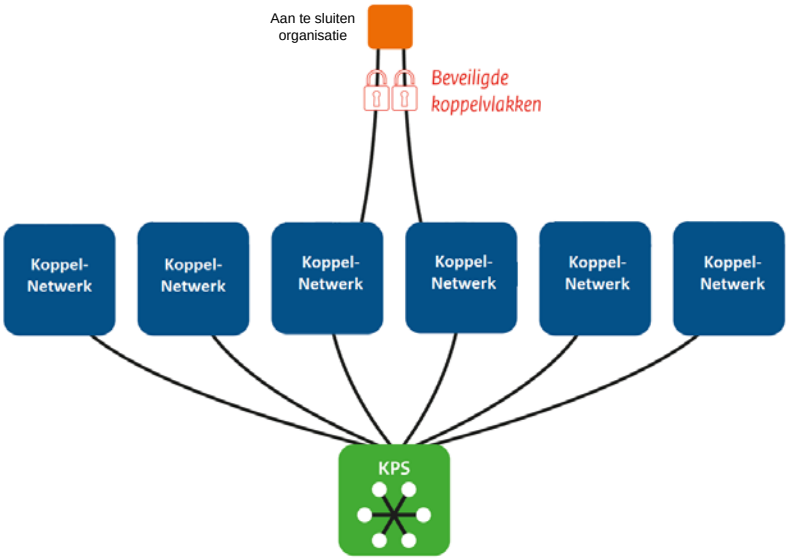
De drie te leveren klantaansluitingen zijn in de volgende tekeningen weergegeven.



Figuur 1: enkelvoudige aansluiting



Figuur 2: redundante aansluiting



Figuur 3: redundante aansluiting op twee koppelnetwerken

Eis 12: Elke aangesloten Organisatie voldoet aan de gemeenschappelijke aansluitvoorwaarden Diginetwerk [2].

5.4 Koppelvlak Koppelnet-KPS

Het koppelvlak tussen een Koppelnetwerk en een KPS is gebaseerd op de gebruikelijke netwerkstandaarden en snelheden. Op laag 1 worden interfaces op koper en glas aangeboden, op laag 2 Ethernet en op laag 3 IP.

Eis 13: Het koppelvlak tussen een Koppelnetwerk en een KPS is gebaseerd op de gebruikelijke netwerkstandaarden en snelheden. Op laag 1 worden interfaces op koper en glas aangeboden, op laag 2 Ethernet en op laag 3 IP.

Routering op het koppelvlak tussen een Koppelnetwerk en een 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 leveranciers niet mogelijk is, kan gebruikt gemaakt worden van private AS-nummers die door Logius worden uitgegeven en geregistreerd. Een Koppelnetwerk en het KPS dienen zowel 16-bit als 32-bit AS-nummers te ondersteunen.

Eis 14: Routering op het koppelvlak tussen een Koppelnetwerk en het KPS is gebaseerd op BGP-4 en gebruikt door RIPE of Logius geregistreerde AS-nummers. Zowel 16-bit als 32-bit AS-nummers dienen ondersteund te worden

Koppelnetwerkbeheerder is verantwoordelijk voor de verbinding van het Koppelnetwerk naar het KPS. De Koppelnetwerkbeheerder plaatst zijn router, onder begeleiding van de KPS leverancier in één van 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.

Eis 15: Koppelnetwerkleveranciers plaatsen hun netwerkapparatuur, waaronder ten minste een IP router, in één van de kasten van het KPS. De beschikbare ruimte is max. 4 hoogte-eenheden.

De koppelnetwerk leverancier dient een IP-router te plaatsen en te verbinden met het laag 2 KPS-netwerk. De IP-adressen voor de koppeling wordt door de KPS-beheerder uit naam van Logius toegewezen. Op de elke KPS verbinding wordt maximaal 1 MAC-adres toegelaten.

Eis 16: Koppelnetwerkleveranciers plaatsen hun netwerkapparatuur, waaronder ten minste een IP-router, in één van de kasten van het KPS. De beschikbare ruimte is max. 4 hoogte-eenheden.

Eis 17: Elk Koppelnetwerk voldoet aan de aansluitvoorwaarden Koppelnet Publieke Sector [3].

5.5 Beheer

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

Omdat in het stelsel 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. Logius heeft hiertoe centrale beheertooling ingericht, welke door de Aangesloten Organisaties, Koppelnetwerken en KPS gebruikt kunnen worden. Essentieel voor het goed functioneren van deze tooling is het kunnen vergaren van informatie van diverse componenten in de verschillende netwerken onder andere door

middel van probes en het gebruik van netwerk protocollen waaronder ping, TCP-connect, SNMP, Syslog, Netflow en/of http queries.

> Eis 18: Koppelnetwerk en KPS leveranciers verplichten zich de centrale beheertooling van Logius van adequate informatie te voorzien. Onder meer door het plaatsen van probes, het sturen van syslog en/of netflow informatie en het toestaan van ping, TCP-connect, SNMP en/of HTTPs queries op relevante apparatuur, waaronder route servers, koppelrouters, DNS servers etc.

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

> Eis 19: Koppelnetwerk- en KPS-leveranciers geven inzicht in de BGP-routering, ping- en traceroute gegevens, door middel van BGP looking glass dat toegankelijk is voor alle deelnemers in het stelsel.

Op de Koppelnetwerken en het KPS is een test-website beschikbaar, waar een http-sessie naar toe gemaakt kan worden. Deze site geeft het IP adres terug van de initiator.

> Eis 20: Koppelnetwerk en KPS-leveranciers stellen een test-website beschikbaar waar een http-sessie naar toe gemaakt kan worden en het IP adres van de initiator teruggeeft.

Voor beheer is het belangrijk dat alle deelnemers in het stelsel 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.

> Eis 21: Deelnemers aan het stelsel dienen maatregelen te nemen, zodanig dat traceroute en PMTUD volledig ondersteund worden.

5.6 Beveiliging

Het basisbeveiligingsniveau van Diginetwerk is semi-vertrouwd conform de NORA definitie.

> Eis 22: Binnen Diginetwerk dient het beveiligingsniveau semi-vertrouwd gehanteerd te worden.

De Aangesloten Organisatie die op Diginetwerk aansluit dient dat via een beveiligd koppelvlak te doen, ongeacht of het klantnetwerk een gelijk, hoger of lager beveiligingsniveau heeft.

> Eis 23: (Klant) organisaties die op Diginetwerk aansluiten dienen dat via een beveiligd koppelvlak te doen.

Een belangrijke functie van Diginetwerk is het transparant transporten van IP-pakketten. Hierom mag er tussen de Koppelnetwerken en een KPS geen blokkerende firewalls of IP-filters aanwezig zijn voor de vastgestelde Diginetwerk IP-reeksen. Op het koppelvlak tussen Koppelnetwerk en een KPS is derhalve geen beveiligd koppelvlak actief.

Eis 24: Op het koppelvlak tussen Koppelnetwerk en een KPS is geen beveiligd koppelvlak actief en worden IP-pakketten transparant getransporteerd.

Om het besloten karakter van Diginetwerk te garanderen mag alleen bekend en vertrouwd verkeer gerouteerd worden, dat wil zeggen dat er uitsluitend IP-verkeer gerouteerd wordt afkomstig van IP-adressen die door Logius voor Diginetwerk zijn vastgesteld en geregistreerd. Indien afwijkend verkeer aangetroffen wordt, dient dit gerapporteerd te worden aan Logius.

Eis 25: Binnen Diginetwerk mag alleen bekend en vertrouwd verkeer gerouteerd worden. Indien onbekend en of onvertrouwd verkeer in Diginetwerk aangetroffen wordt, dient dit gerapporteerd te worden.

Koppelnetwerk leveranciers zijn verplicht om uitgaand verkeer naar een KPS te controleren op source-IP adressen en pakketten met een source-IP adres dat niet tot hun koppelnetwerk behoort te verwijderen (anti-spoofing protectie). KPS leveranciers zorgen ervoor dat geen IP routes/prefixes geïnjecteerd worden die niet toegestaan zijn.

Eis 26: Koppelnetwerk leveranciers zijn verplicht anti-spoofing protectie toe passen op het koppelvlak met een KPS.

Eis 27: KPS leveranciers zorgen ervoor dat er geen IP routes/prefixes in BGP geïnjecteerd of verspreid worden die niet behoren tot de IP adressen in Diginetwerk.

5.7 Minimale technische specificaties

In deze paragraaf staan de technische specificaties benoemd waaraan het koppelvlak tussen Koppelnetwerk en het KPS minimaal moet voldoen.

Koppelnetwerk en KPS leveranciers ondersteunen minimaal onderstaande standaarden:

- Koper op basis van IEEE 802.3 1000BASE-T
- Multimode glasvezel op basis van IEEE 802.3 1000BASE-SX en 10GBASE-SR.

In alle gevallen wordt gebruik gemaakt van auto-negotiate en full duplex.

Eis 28: Koppelnetwerk en KPS leveranciers ondersteunen minimaal 1000BASE-T, 1000BASE-SX en 10GBASE-SR over multimode glasvezel. In alle gevallen wordt gebruik gemaakt van auto-negotiate en full duplex

Koppelnetwerk en KPS leveranciers mogen additionele standaarden overeenkomen, Logius kan de set minimaal te ondersteunen standaarden aanpassen als er vraag naar is (bijvoorbeeld hogere bandbreedte).

De Koppelnetwerken moeten pakketten met een Ethernet MTU van minimaal 1500 bytes kunnen transporteren, bij voorkeur wordt een Ethernet MTU van 9000 bytes ondersteund. KPS ondersteunt standaard een Ethernet MTU van 9000 bytes.

Eis 29: Koppelnetwerk-leveranciers 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

6 Referenties

[1] Nederlandse Overheid Referentie Architectuur

De volgende documenten zijn te vinden op Logius website:
https://www.logius.nl/diensten/diginetwerk/documentatie

[2] Aansluitvoorwaarden Diginetwerk

[3] Aansluitvoorwaarden Koppelnet Publieke Sector

[4] Dossier Afspraken en Procedures Diginetwerk

[5] Overheidsbreed IPv6-nummerplankader

7 Terminologie

Terminologie die in dit document zijn gebruikt.

Term	Uitleg
AO	Aangesloten Organisatie
AoD	Aansluiting op Diginetwerk
AS	Autonomous System
AZ	Ministerie van Algemene Zaken
BGP	Border Gateway Protocol
BIR	Baseline Informatiebeveiliging Rijksoverheid
DCI	Data Center Interconnect
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DMZ	Demilitarized zone
EAR	Enterprise Architectuur Rijksoverheid
FQDN	Fully Qualified Domain Name
GE	Gigabit Ethernet
GEMMA	Gemeentelijke Model Architectuur
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPS/IDS	Intrusion prevention systems / Intrusion Detection System
ISO/IEC	International Organization for Standardization / International Engineering Consortium
KEC	Koppelvlak Externe Communicatie
KPS	Koppelnet Publieke Sector
NAFIN	Netherlands Armed Forces Integrated Network
NORA	Nederlandse Overheid Referentie Architectuur
ODC	OverheidsDataCenter
OSB	OverheidsServiceBus
PKI	Public Key Infrastructure
PSA	Project Start Architectuur
QoS	Quality of Service
RINIS	Routeringsinstituut (inter)nationale informatiestromen
RIPE	Réseaux IP Européens
RIR	Regional Internet Registry
RON	Rijksoverheidsnetwerk
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNO	Service Niveau Overeenkomst
s-Testa	Secure-Trans European Services for Telematics between Administrations
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VIR-BI	Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie http://wetten.overheid.nl/BWBR0033507
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAN-I	Wide Area Network Interconnect
ZBO	Zelfstandig bestuursorgaan