# Gemeentelijke Gemeenschappelijke Infrastructuur

## Generieke toelichting Diginetwerk voor leveranciers

Versie 1.2
25 november 2020

## Colofon

*GGI - Generieke toelichting netwerkinfrastructuur voor leveranciers*
GGI@vng.nl

## Inhoud



# 1. Inleiding

Een hoogwaardige Nederlandse digitale infrastructuur is meer dan ooit onmisbaar voor de economie en samenleving. Gemeenten moeten blindelings kunnen vertrouwen op alle middelen die ervoor zorgen dat hun burgers veilig en eenvoudig hun zaken kunnen regelen. De Generieke Digitale Infrastructuur (GDI) van de overheid regelt het veilig en betrouwbaar inloggen voor Nederlandse burgers en bedrijven bij de (semi-)overheid en regelt de beschikbaarheid van een aantal basisgegevens voor het gebruik in overheidsprocessen.

Binnen de GDI is DIGINETWERK de standaard die zorgt voor één besloten digitale infrastructuur, waarbinnen veilige en eenvoudige gegevensuitwisseling plaatsvindt voor en tussen Nederlandse organisaties met een publieke taak. De overheid roept ook leveranciers op om aan te sluiten op en gebruik te maken van Diginetwerk. Zo ontstaat een betrouwbare en veilige omgeving voor uitwisseling van gegevens en gebruik van ICT-toepassingen.

De voordelen hiervan zijn:

- Door het besloten karakter is Diginetwerk een veiliger alternatief dan het open internet voor het uitwisselen van gegevens tussen overheidsorganisaties.
- Met één netwerkaansluiting efficiënt en betrouwbaar communiceren met alle aangesloten overheidsorganisaties en andere aangesloten organisaties.

Kortom, door deze gemeenschappelijke basis wordt het samenwerken voor gemeenten onderling en met andere overheden en samenwerkingspartners beter, veiliger en gemakkelijker. Voor commerciële (cloud-)leveranciers is het onder voorwaarden ook mogelijk hun diensten te ontsluiten via Diginetwerk. Hiermee worden verbindingen met deze leveranciers eenvoudiger, kunnen gemeenten meer grip krijgen op hun aanbod en hebben cloudleveranciers een gestandaardiseerde en veilige manier om overheidsklanten op hun diensten aan te sluiten.

# 2. Generieke principes GGI

De generieke principes van GGI :

- De GGI vormt de basis van een gemeentelijke community cloud infrastructuur.
- Vanuit gemeentelijk perspectief reduceert de levering van diensten via Diginetwerk de complexiteit van de benodigde netwerkinfrastructuur voor de uitvoering van de gemeentelijke taken.

- De dienstverlening voor de op Diginetwerk aan te sluiten partijen is nauwkeurig beschreven en transparant.
- Parallel aan het stimuleringsproject om diensten via Diginetwerk te leveren wordt er gewerkt aan het verbeteren van standaardisatie van diensten door Cloud-Afspraken op te stellen. Cloud-Afspraken omvatten de aanvullende regels en afspraken die gemeenten hanteren voor de levering en het gebruik van clouddiensten. Cloud-Afspraken zijn onderdeel van het stelsel van overeenkomsten en afspraken dat is gebaseerd op GIBIT. Deze afspraken worden aan de GIBIT toevevoegd, VNG verwacht eind 2020 een eerste set afspraken beschikbaar te kunnen stellen.
- Het koppelnet voor gemeenten, GGI-Netwerk, staat volledig onder zeggenschap van gemeenten.
- Diginetwerk wordt op basis van het IPv6 overheidsnummerplankader ingericht maar ondersteunt ook IPv4. Beide standaarden worden hier vanuit functioneel oogpunt expliciet genoemd vanwege de noodzaak om de toegankelijkheid tussen gemeenten en de buitenwereld te kunnen waarborgen.

# 3. Ontwerp principes

Diginetwerk is een afsprakenstelsel voor het koppelen van besloten netwerken van de overheid. De gekoppelde besloten netwerken (bekende trusted partijen) maken uitwisseling van gegevens tussen overheden mogelijk en vormen een veiliger alternatief t.o.v. connecties via het open internet.

Een koppelnetwerk fungeert door middel van de aansluiting op het Koppelpunt Publieke Sector (KPS) als koppelvlak tussen Diginetwerk en de bedrijfsnetwerken van aangesloten organisaties. Vanuit de Diginetwerk-architectuur bezien moet ieder te koppelen bedrijfsnetwerk voldoen aan de eisen, die gesteld worden in de Aansluitvoorwaarden Diginetwerk[1] van Logius, de beheerder van het Afsprakenstelsel Diginetwerk. Met de aansluiting op Diginetwerk heeft een organisatie connectiviteit naar alle aangesloten (landelijke) voorzieningen, partijen en andere overheden.

Voor de aansluiting op Diginetwerk stelt Logius de volgende eisen:

- Een aansluiting dient te voldoen aan de randvoorwaarden zoals vastgelegd in de Aansluitvoorwaarden Diginetwerk.
- De aansluiting is een overgang van Diginetwerk naar een ander beveiligingsniveau en er dient derhalve een beveiligd koppelvlak gebruikt te worden dat logging en inspectie mogelijk maakt.
- De aansluitende organisatie is zelf verantwoordelijk voor de beveiligingsmaatregelen op hun aansluiting op Diginetwerk.
- Diginetwerk is transparant voor het transport van IP-pakketten.
- Het gebruik van Internet-VPN's binnen Koppelnetwerken Diginetwerk[2] en voor klantaansluitingen is niet toegestaan.
- Er mag vanuit Diginetwerk geen communicatie van en naar het internet mogelijk zijn.
- Er mogen tussen een koppelnetwerk en het KPS geen blokkerende firewalls aanwezig zijn voor regulier gebruikersverkeer (HTTP, HTTPS, DNS, SMTP, ICMP, NTP).
- Vanuit het Koppelnetwerk worden uitsluitend IP-protocollen op het KPS aangeboden.
- Tussen de koppelnetwerken die aangesloten zijn op het KPS wordt IP-verkeer onderling dynamisch gerouteerd met de door Logius vastgestelde BGP-standaard (BGP-4).
- Voor gebruik van het BGP-protocol dient de beheerder van het koppelnetwerk te beschikken over een Autonomous Sytem Number. Toegestaan zijn:

[1] https://www.logius.nl/sites/default/files/public/bestanden/diensten/DigiNetwerk/Aansluitvoorwaarden-Diginetwerk.pdf
[2] Hier wordt bedoeld dat Internet-VPN's geen onderdeel mogen zijn van een Koppelnetwerk, IP-VPN's over Diginetwerk zijn wel toegestaan.

    - publieke AS-numbers die door het RIPE NCC (of één van de andere RIR's) aan de betreffende organisatie uitgegeven zijn (deze optie heeft de voorkeur), of
    - private AS-numbers die door Logius uitgegeven en geadministreerd worden.
- Apparatuur dient 32-bit (4-byte) AS-numbers te ondersteunen.
- Er wordt uitsluitend IP-verkeer gerouteerd afkomstig van die IP-adressen die door Logius zijn verstrekt (via de koppelnetwerkbeheerder) en geregistreerd.
- ICMP-pakketten van type "Fragmentation Needed and Don't Fragment was Set" (type 3, code 4) dienen waar nodig door routers te worden gegenereerd en niet uitgefilterd.
- Het Ethernetverkeer wordt door de Koppelnetwerkbeheerder op basis van de IEEE 802.3-standaard en RFC 894 aangeboden.
- Koppelnetwerkbeheerders zijn verplicht om van hun koppelnetwerk richting KPS uitgaand verkeer te controleren op source IP-adressen, en pakketten met een source IP-adres dat niet tot hun koppelnetwerk behoort te verwijderen alvorens het aangeboden wordt aan het KPS (anti-spoofing protectie).
- De Koppelnetwerkbeheerder is binnen zijn netwerk verplicht voor alle IP-interfaces, die deel uitmaken van een routeerbaar pad door Diginetwerk, ICMP/UDP-verkeer zodanig te ondersteunen dat alle andere Koppelnetwerkbeheerders door middel van een Traceroute het volledige routeerbare pad kunnen bepalen.

## 3.1. Beschikbaarheid

De beschikbaarheid van de dienstverlening wordt bepaald door de beschikbaarheid van de centrale en lokale componenten.

**Centrale inrichting**

- Diginetwerk is 7 x 24 uur beschikbaar met een beschikbaarheidseis van >99,9%.
- Diginetwerk is opgebouwd met redundante aansluitingen met een automatische herroutering.

**Lokale inrichting**

- Organsiaties kunnen bij hun aansluiting op Diginetwerk de keuze maken tussen een enkelvoudige en een redundante configuratie. Voor een redundante aansluiting dienen twee gescheiden accessen te zijn aangelegd en dient er een keuze gemaakt te worden voor het failover-mechanisme.

## 3.2. Beveiliging

Diginetwerk is een beveiligingsmaatregel op zich. Het netwerk kent een besloten karakter. Er is geen directe (d.w.z. zonder beveiligde ontkoppeling) koppeling met openbare netwerken zoals internet mogelijk of aanwezig.
Diginetwerk is een infrastructuur voor datatransport. Encryptie, identificatie en authenticatie kunnen op applicatieniveau ingeregeld worden.

**Afsprakenstelsel Diginetwerk**

Ieder koppelnetwerk is onderdeel van het afsprakenstelsel Diginetwerk en voldoet dus aan de beveiligingseisen van Diginetwerk. VNG Realisatie heeft GGI-Netwerk ingericht conform de door Logius aan Diginetwerk Koppelnetwerken gestelde beveiligingseisen. Bij oplevering van GGI-Netwerk is hierop een controle gedaan door Logius.

**Aansluitende partijen**

Partijen, die aansluiten op Diginetwerk, moeten voldoen aan de Aansluitvoorwaarden Diginetwerk en de daarin gestelde voorwaarden aan de beveiliging van de aansluiting. Er wordt gekoppeld middels beveiligde

koppelvlakken: op Diginetwerk kunnen besloten netwerken aangesloten worden met een ander (zowel hoger of lager) beveiligingsniveau. Hiervoor geldt de verplichting dat er op het koppelvlak en aan de klantzijde een beveiligingsfunctie actief is (beveiligd koppelvlak).
Conform het afsprakenstelsel Diginetwerk is de aangesloten organisatie zelf verantwoordelijk voor de beveiligingsmaatregelen op hun aansluiting.
Een organisatie zal zijn elektronische communicatienetwerk en zijn aansluiting op Diginetwerk moeten beveiligen conform de informatiebeveiligingstandaarden NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002 om te voldoen aan de Aansluitvoorwaarden Diginetwerk.

**Penetratietesten en Security-monitoring**
Koppelnetbeheerders geven opdracht voor het uitvoeren van penetratietesten om de conformiteit met de beveiligingseisen te controleren.

### 3.3. DNS

Aangesloten organisaties op Diginetwerk kunnen gebruikmaken van het Rijks-DNS voor het resolven van domeinnamen, die eindigen op diginetwerk.net en diginetwerk.nl. Van services, die aangesloten partijen op Diginetwerk aan de gebruikers ter beschikking willen stellen, kunnen de domeinnamen (onder diginetwerk.net of diginetwerk.nl) eveneens in het Rijks-DNS geregistreerd worden.

# 4. Aangesloten koppelnetwerken

De besloten netwerken die onderdeel zijn van Diginetwerk noemen we koppelnetwerken. De Koppelnetwerken zijn gekoppeld via het Koppelnet Publieke Sector (KPS).
In het online overzicht op de website van Logius vindt u de beschikbare aanbieders van koppelnetwerken.
De aanbieders dienen zich te houden aan de aansluitvoorwaarden Koppelnet Publieke Sector. U bepaalt zelf bij welk koppelnetwerk uw organisatie zich aansluit. Desgewenst kunt u hierover met Logius overleggen.

# 5. Stappenplan aansluiting op Diginetwerk

**Stap 1: Aanvragen Diginetwerkaansluiting**
- De coördinatie van de aansluiting ligt bij uzelf.
- Als u nog geen aansluiting heeft op een koppelnetwerk, neem dan contact op met de aanbieder van het door u gekozen koppelnetwerk. Logius kan u adviseren bij de keuze voor het koppelnetwerk.
- U ondertekent de Aansluitvoorwaarden Diginetwerk als onderdeel van de overeenkomst met de koppelnetwerkaanbieder.
- Hier vindt u het Diginetwerk aanvraagformulier voor leveranciers dat u dient in te vullen en op te sturen; op basis hiervan zal Logius toestemming geven voor de Diginetwerkaansluiting.

**Stap 2: Inrichten Diginetwerkaansluiting**
- De koppelnetwerkaanbieder kent u een Diginetwerk IP-adresreeks toe voor uw aansluiting. Het IP-adres is uw digitale huisnummer binnen Diginetwerk.

- U maakt het implementatieplan en stelt een vaste contactpersoon aan die de inrichting van de aansluiting op Diginetwerk begeleidt vanuit uw organisatie. Dit kan bijvoorbeeld een projectleider of implementatiecoördinator zijn.

**Stap 3: Opleveren Diginetwerkaansluiting**

- In samenwerking met de koppelnetwerkaanbieder doorloopt u een acceptatietest.
- Bij goed doorlopen van de acceptatietesten tekenen beide partijen het acceptatietestdocument en gaat uw aansluiting in productie.

Stap 4:

- U selecteert een eerste klant om de verbinding met uw toepassing via Diginetwerk te realiseren.
- Na een succesvolle eerste implementatie kunt u de mogelijkheid van ontsluiting via Diginetwerk breder naar uw klanten communiceren. Geef dit ook door aan VNG Realisatie, dan wordt dit ook opgenomen in de documentatie over GGI.

# Contact

GGI@vng.nl: voor meer informatie over GGI
https://www.logius.nl/diensten/diginetwerk: voor documentatie over Diginetwerk